

2 RS
1c520 U.S. PTO
09/801557
03/08/01

THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of : Mitsuaki KAKEMIZU, et al.

Filed : Concurrently herewith

For : MULTIMEDIA SIGNAL PROCESSING APPARATUS

Serial No. : Concurrently herewith

March 8, 2001

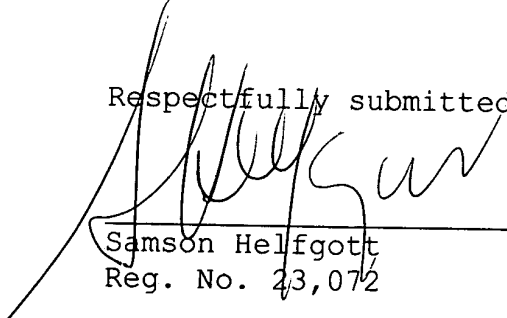
Assistant Commissioner of Patents
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Attached herewith are Japanese patent application No.
2000-225857 of July 26, 2000 whose priority has been claimed in
the present application.

Respectfully submitted



Samson Helfgott
Reg. No. 23,072

HELFGOTT & KARAS, P.C.
60th FLOOR
EMPIRE STATE BUILDING
NEW YORK, NY 10118
DOCKET NO.: FUJA 18.427
BHU:priority

Filed Via Express Mail
Rec. No.: EL522402279US
On: March 8, 2001
By: Brendy Lynn Belony
Any fee due as a result of this paper,
not covered by an enclosed check may be
charged on Deposit Acct. No. 08-1634.

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 7月26日

出 願 番 号

Application Number:

特願2000-225857

出 願 人

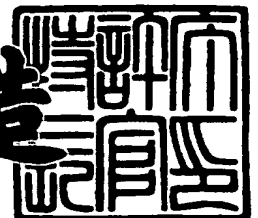
Applicant(s):

富士通株式会社

2000年10月20日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3087438

【書類名】 特許願

【整理番号】 0051355

【提出日】 平成12年 7月26日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 H04L 12/56
H04Q 7/36
G09C 1/00

【発明の名称】 モバイル I P ネットワークにおける V P N システム及び
V P N の設定方法

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 掛水 光明

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜 2 丁目 2 番 1 号 富士通西日
本コミュニケーション・システムズ株式会社内

【氏名】 山村 新也

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 五十嵐 洋一郎

【発明者】

【住所又は居所】 福岡県福岡市早良区百道浜 2 丁目 2 番 1 号 富士通西日
本コミュニケーション・システムズ株式会社内

【氏名】 村田 一徳

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 若本 雅晶

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100077517

【弁理士】

【氏名又は名称】 石田 敬

【電話番号】 03-5470-1900

【選任した代理人】

【識別番号】 100092624

【弁理士】

【氏名又は名称】 鶴田 準一

【選任した代理人】

【識別番号】 100100871

【弁理士】

【氏名又は名称】 土屋 繁

【選任した代理人】

【識別番号】 100082898

【弁理士】

【氏名又は名称】 西山 雅也

【選任した代理人】

【識別番号】 100081330

【弁理士】

【氏名又は名称】 樋口 外治

【手数料の表示】

【予納台帳番号】 036135

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9905449

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 モバイル I P ネットワークにおける V P N システム及び V P N の設定方法

【特許請求の範囲】

【請求項 1】 I P ネットワーク上で端末がネットワーク間を移動したときに、I P アドレスの管理と移動先への通信パケットの転送を自動化したプロトコルを用いたネットワークのホームネットワークに設けられるサーバ装置において

前記端末と関連つけて、I P ネットワーク内に安全な通信路を構築するための情報を記憶する記憶手段と、

移動先の外部ネットワーク内の前記端末と、前記端末と通信を行う相手先端末との間に安全な通信路を構築できるように前記情報を分配する分配手段とを設けたことを特徴とするサーバ装置。

【請求項 2】 前記分配手段は、相手先端末のある外部ネットワークのルータへ前記情報を転送することを特徴とする請求項 1 に記載のサーバ装置。

【請求項 3】 前記安全な通信経路は仮想プライベート・ネットワークで実現される通信路であり、前記情報は前記仮想プライベート・ネットワークとしての設定経路情報とセキュリティ情報を含む情報であることを特徴とする請求項 1 に記載のサーバ装置。

【請求項 4】 前記分配手段は、前記端末からの位置登録要求メッセージに対する認証応答メッセージ送出時に、前記情報を分配することを特徴とする請求項 1 に記載のサーバ装置。

【請求項 5】 前記分配手段は、通信先となる相手先端末からの通信パケットを受け取った後に、前記情報を分配することを特徴とする請求項 1 に記載のサーバ装置。

【請求項 6】 モバイル I P ネットワークにおける V P N システムは、移動端末と、ユーザのホームネットワークに設けられたホーム認証サーバとそれ以外の外部ネットワークに設けられた外部認証サーバと、

ホームネットワークに設けられたVPNデータベースと、
ホームネットワーク、外部ネットワーク、及び所定の通信ホスト及び／又はその代理サーバの各ゲートウェイ機能を有するネットワーク装置と、
で構成され、

ホーム認証サーバは、移動端末からの位置登録要求時に認証を要求したユーザのVPN情報をVPNデータベースから抽出し、そのVPN情報を所定の位置登録メッセージ及び認証応答メッセージを用いて各ネットワーク装置に通知し、

各ネットワーク装置は、通知されたVPN情報を基にホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間にそれぞれIPSecによるVPNパスを設定する、ことを特徴とするVPNシステム。

【請求項7】 認証サーバ及びネットワーク装置は、移動端末の移動による位置登録要求と連動して認証サーバ及びネットワーク装置にキャッシュされたVPN情報を新経路情報に更新するか、又はモバイルIPで通知される位置情報で書き換えることにより、ホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間の各VPNパスを新たなIPSecによるVPNパスに自動更新する、請求項6記載のシステム。

【請求項8】 ホーム認証サーバは、

前記VPNデータベースのVPN情報と、自身が保有すると通信先ホストを収容する所定のネットワーク装置との対応表を用い、所定の認証要求メッセージに設定された移動端末が接続した外部ネットワーク装置の情報と移動端末のホームネットワーク装置の情報からVPN設定経路を特定するAAAVPN制御部と、

各ネットワーク装置間のサービス品質とセキュリティ情報をサービスプロファイルとして、アクセスネットワークへの所定の認証応答メッセージ及びホームネットワークへの位置登録メッセージに設定するAAAプロトコル処理部と、
を有する請求項6記載の装置。

【請求項9】 各ネットワーク装置は、

キャッシュによりVPN情報が設定されたサービスプロファイルに関連するプ

ロトコル群を制御するMAプロトコル処理部と、

そのサービスプロファイルに従ってサービス品質を保証するQoS制御とセキュリティゲートウェイ間のセキュリティを保証するためのトンネルを設定するMAVPN制御部と、

を有する請求項6記載の装置。

【請求項10】 モバイルIPネットワークにおけるVPNの設定方法は、

ー ユーザの移動端末から外部エージェントに位置登録要求メッセージを送信すること、

ー 外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

ー ホーム認証サーバは、受信した認証要求メッセージより自身のデータベースを参照して通信先ホスト、ネットワーク装置種別、及びユーザ別のセキュリティ・サービス情報を抽出し、ネットワーク装置種別がVPN動的設定可である場合はVPNキャッシュに外部エージェントー通信先ネットワーク装置のVPNを設定して、それらの情報を含む位置登録要求メッセージをホームエージェントに送信すること、

ー ホームエージェントは、受信した位置登録要求メッセージをキャッシュし、位置登録処理の終了後にネットワーク装置種別がVPN動的設定可である場合は通信先ホスト宛にこのVPN情報を付加した結合更新メッセージを送出すること、

ー ネットワーク装置は結合更新メッセージを代理受信し、それに付加されたVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、ネットワーク装置から外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、その後に結合承認メッセージをホームエージェントに送信すること、

ー ホームエージェントは、結合承認メッセージを受信すると、位置登録応答メッセージをホーム認証サーバへ送信すること、

ー ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュ

してある外部エージェントーネットワーク装置間のVPN情報を付加した認証応答メッセージを外部エージェントのローカル認証サーバに送信すること、

ー ローカル認証サーバは、受信した認証応答メッセージをその付加されたVPN情報をキャッシュしてから外部エージェントへ送信すること、

ー 外部エージェントは、受信した認証応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、外部エージェントからネットワーク装置に向けたIPSecトンネルによるVPNパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、

から成ることを特徴とするVPNの設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

近年インターネットの普及に伴い、企業の専用線をインターネット上の仮想パス（VPN：Virtual Private Network）で置き換える事により、通信コストを低減しようとする試みが広く行われるようになってきている。また、電子商取引を実現する上でもインターネット上のセキュリティ強化は必須であり、これらを実現する技術としてIP Security Protocol（以降、「IP Sec」と称す）が注目されている。

【0002】

一方、IMT-2000の本格導入をまじかに控え、インターネット環境はモバイル環境への移行が始まっている。モバイル環境をインターネットへ導入することはそれを利用するユーザの利便性を高める。しかしながら、その一方でセキュリティを脆弱にする危険性も増大させることになり、モバイル環境でセキュリティを保護する枠組みが求められている。

【0003】

IMT-2000でコアネットワークアーキテクチャの基礎となるRFC2002で規定されたIP Mobility Support（以降、「モバイルIP（Mobile IP）」と称す）にIPSecを組み合わせる方式についても、いくつかの提案がされている。ここで、モバイルIP（mobile internet protocol）

とは、IPネットワーク上で端末がネットワーク間を移動した時に、IPアドレスの管理と移動先への通信パケットの転送を自動化した技術である。ルータにアドレスの転送を実行するエージェント機能を実装し、端末の“本籍”にあたるホーム・アドレスと現住所の“気付アドレス”の2つを管理させる。端末は、ネットワーク間を移動した際に新しい気付アドレスを、ホーム・アドレスのあるネットワークのルータに登録し、移動を知らない通信相手からのメッセージをトンネリング技術で転送させる。

【0004】

しかしこれらの提案は、通信経路上（具体的にはホームエージェントと通信端末との間）の完全なセキュリティを保証していないために、エンドユーザ端末がIPSec機能を持つことを前提としている。これらの提案では、結局通信に参与する端末が全てIPSecを実装する必要があり、モバイル環境でセキュリティを保護する枠組みとしては、不十分であり、モバイルIPとIPSecとを連携させる意義が薄い。

【0005】

【従来の技術】

図1は、既存の提案によるモバイルIP+IPSecを適用したネットワーク構成の一例を示したものである。

ここでは、モバイル環境をサポートするIPアーキテクチャとしてRFC2002で提案されたモバイルIPと、インターネット上でセキュリティを実現するアーキテクチャであるIPSecとを併用している。モバイルIPは、その本質から通常のネットワークに比較してセキュリティ面が脆弱なため、IPSecを含む様々なセキュリティ強化の方式がとりいれられている。

【0006】

図1の例では、モバイルIPで規定されるユーザ1（MN:Mobile Node）がアクセスしたネットワーク2にある移動性エージェント21（外部エージェントFA:Foreign Agent）とユーザのホームネットワーク3にある移動性エージェント31（ホームエージェントHA:Home Agent）との間におけるIP-IPトンネルをIPSecトンネル6で置き換えるものであり、IPSecで用いるVPN

用の情報はあらかじめ各移動性エージェント 2 1 及び 3 1 に設定しておく必要がある。

【0 0 0 7】

動的に I P S e c トンネル 7 を設定することについてもこれらの提案で触れているが、移動端末 1 と移動性エージェント 2 1、3 1 との間の自動鍵交換 (I K E) に頼った方式であり、通信先ホスト 5 2 (C N : C o r e s p o n d e n t N o d e) ととも自動鍵交換 (I K E) を用いて個別に I P S e c を設定する必要がある。この場合、さらにモバイル I P の変更も必要となる。

【0 0 0 8】

一般に、VPN は I P S e c や M P L S 等を用いてインターネット上に張られるユーザの仮想パスのことを言うが、他のインターネット技術、例えば D i f f e r e n t i a t e d S e r v i c e (以降、「差別化サービス」と称す) 等、とユーザ単位では連携しておらず、その結果 VPN のサービス品質保証は十分なネットワーク資源の割当てと一律な優先制御 (例えば、I P S e c プロトコルのプロトコル番号をフィルタリング条件とした簡単な優先度制御) とによって行われている。

【0 0 0 9】

【発明が解決しようとする課題】

上記で述べたような方式によれば、結局は通信に関与する端末が全て I P S e c を実装する必要がある。そのため、ネットワークとして I P S e c サービスを提供する意義が薄く、またセキュリティサービスとサービス品質保証とを自由に組み合わせてユーザの利便性を向上させたネットワークサービスを、I P S e c を実装していない既存の端末を含めて、提供することが出来ないという問題があった。

【0 0 1 0】

本発明の目的は、モバイル I P における通信を安全な通信経路を用いて可能にすることにある。また、本発明の目的は、モバイル I P における位置登録手順と連携して、通信に関与する端末の公衆 I P ネットワークへのセキュリティゲートウェイに動的に I P S e c を用いた VPN を設定することによって、移動端末や

通信端末にVPN用の特殊な機能を持たせること無く任意の端末間での通信にVPN設定サービスを提供し、ユーザの利便性向上させたVPNサービスを提供することにある。それにより、VPNサービスを提供するサービスプロバイダの差別化も可能になる。

【0011】

より具体的には、以下のことを目的とする。

1) モバイルIPにおける位置登録手順と連携して、通信に關与する端末の公衆IPネットワークへのセキュリティゲートウェイ21、31に動的にIPSecを用いたVPNを設定することで、MN1やCN42、52にVPN用の特殊な機能を持たせること無く、任意の端末間でのVPN設定サービスの提供を可能にする。

2) ユーザが自由に組み合わせて指定したサービス品質、セキュリティレベル、経路でのVPN設定を可能にする。

3) MN1の移動に伴い、VPNの経路を自動更新することを可能にする。

【0012】

【課題を解決するための手段】

図2には、図1の構成と対比させた本発明に基くネットワーク構成例を示しており、モバイルIPにおける位置登録手順と連携して、通信に關与する端末の公衆IPネットワーク2～5の各セキュリティゲートウェイ21～51に動的にIPSecを用いたVPNを設定することで任意の端末1やホスト32～52間の通信にVPN設定サービスを提供する。

【0013】

図3は、本発明の基本的な機能ブロック構成例を示したものである。

最初に、以降で使用される用語の簡単な説明を行なっておく。MIP (Mobile IP) は、RFC2002と将来の全ての拡張で規定されるモバイルIPプロトコルである。AAAプロトコルは、AAAシステムが使用するプロトコルであって、本願の実施例では現在IETFで検討中のDIAMETERプロトコルの使用を想定している。AAAプロトコルは認証(Authentication)、認可(Authorization)、課金(Accounting)、及びポリシーに関する情報を伝達可能なあらゆるブ

ロトコルで実装可能である。本発明で必要となる新たな情報の伝達には前記 D I A M E T E R プロトコルで定義される A V P (Attribute Value Pair) と呼ばれる拡張可能な属性パラメータを用いる。拡張される属性は V P N 設定に関する情報である。

【 0 0 1 4 】

MN (Mobile Node) は、モバイル I P プロトコル機能を有する移動端末を示す。A A A は、上述した認証、認可、課金を行うサーバ群の I E T F で用いられる名称である。A A A H は認証要求ユーザーの加入者データを持つネットワークの A A A であり、A A A F は該ユーザーの加入者データを持たないネットワークの A A A である。本発明の A A A は上記機能に加えて V P N データベースから認証要求ユーザの V P N 情報を抽出し、H A へ H A 登録要求メッセージで、また F A へは A A A F を経由した認証応答メッセージで V P N 情報を通知し、さらにユーザ単位の V P N 情報の抽出と V P N 経路の決定を行う。

【 0 0 1 5 】

F A (Foreign Agent) は、R F C 2 0 0 2 で定義される機能エンティティであって移動端末に割り付けられるホームアドレスを所有しないエージェントである。自ノードのアドレスである気付アドレス (Care-of-Address) にカプセル化されて送られてきたパケットをデカプセル化し、ホームアドレスに対応したリンクレイヤアドレスへ回送する。このアドレスの対応は、訪問者リストと呼ばれるテーブルで管理される。本発明の F A は I P S e c のセキュリティゲートウェイ機能と差別化サービスのエッジルータ機能とを兼ね備える。

【 0 0 1 6 】

H A (Home Agent) は、R F C 2 0 0 2 で定義される機能エンティティであって移動端末に割り付けられたホームアドレスを所有するエージェントである。H A に回送されてきた移動端末のホームアドレスを送信先とするパケットはホームアドレスに対応した F A の気付アドレスへカプセル化されて送出される。このアドレスの対応は移動結合と呼ばれるテーブルで管理される。本発明の H A は I P S e c のセキュリティゲートウェイ機能と差別化サービスのエッジルータ機能を兼ね備える。

【 0 0 1 7 】

PCN (Proxy Correspondent Node) は、特許 2 0 0 0 - 3 2 3 7 2 号で規定された機能エンティティであって配下のモバイル IP をサポートしない通信ノード (CN ; Correspondent Node) に代わって、HA から送られてきた CN への結合更新メッセージを代理受信し、結合更新で通知された宛先へ結合トンネルを設定する。本発明の PCN は IPsec のセキュリティゲートウェイ機能と差別化サービスのエッジルータ機能を兼ね備えており、MIP プロトコルで通知される VPN 情報を解析し、その解析した VPN 情報に基づいてネットワークカーネルに差別化サービスの設定と指定されたセキュリティレベルでのトンネルを設定する。

【 0 0 1 8 】

本発明によれば、モバイル環境をサポートする IP ネットワークは、ユーザ認証サーバ及びネットワーク装置で構成され、移動端末 1 からの初回位置登録要求 (認証要求) 時に、認証サーバ (AAAH) が認証を要求したユーザの VPN 情報を VPN データベースから抽出し、その VPN 情報を位置登録メッセージ及び認証応答メッセージを用いてネットワーク装置 (HA, FA) に通知する。ネットワーク装置 (HA, FA) は、通知された VPN 情報を基に HA と FA 間に VPN を設定する。その際、ネットワーク装置 (HA) は、通信先端末 CN が他のネットワーク 4 に存在する場合は更に HA から VPN 情報で指定された通信先端末収容のセキュリティゲートウェイ (PCN) へ VPN を設定する。

【 0 0 1 9 】

また、前記認証サーバ及びネットワーク装置は、移動端末 1 の移動による位置登録要求と連動して認証サーバ及びネットワーク装置にキャッシュされた VPN 情報を新経路情報に更新するか又はモバイル IP で通知される位置情報で書き換える。その結果、新 FA と HA 間及び PCN と新 FA 間に新たな IPsec トンネルが動的に設定され、VPN 経路が自動更新される。さらに、FA 間のデータパケット転送におけるセキュリティ保護を完全なものとするため、スムーズハンドオフ時の FA 間の結合トンネルにも IPsec トンネルが設定される。

【 0 0 2 0 】

本発明の認証サーバ（A A A H）は、ユーザが所望するサービス品質、セキュリティゲートウェイ間のセキュリティ情報、及びV P Nを設定する通信先ホスト（C N）のI Pアドレス群からなるユーザ単位のV P N情報と通信先ホストを収容するセキュリティゲートウェイ（V P N G W）との対応表を格納するV P Nデータベースと、認証要求メッセージに設定された移動端末が接続したアクセスネットワーク2のセキュリティゲートウェイ（F A）アドレスと移動端末のホームネットワーク3のセキュリティゲートウェイ（H A）アドレス、及び前記ユーザ対応V P N情報に設定された通信先ホスト（C N）と前記対応表から抽出される通信先ホストを収容するセキュリティゲートウェイ（P C N ; Proxy C N）アドレスからV P N設定経路を特定するA A A V P N制御部と、各セキュリティゲートウェイ間のサービス品質とセキュリティ情報をサービスプロファイルとして、アクセスネットワークへの認証応答メッセージ及びホームネットワークへの位置登録メッセージに設定するA A Aプロトコル処理部と、を有する。

【 0 0 2 1 】

また本発明のセキュリティゲートウェイから成るネットワーク装置（H A、F A、P C N）は、上記V P N情報を設定されたサービスプロファイルとR F C 2 0 0 2とそれに関連するその他の拡張プロトコルを理解するためのM A (M o b i l i t y A g e n t)プロトコル処理部と、通知されたサービスプロファイルに従いサービス品質を保証するQ o S制御とセキュリティゲートウェイ間のセキュリティを保証するためのトンネルを設定するM A V P N制御部と、を有する。

【 0 0 2 2 】

前記M Aプロトコル処理部は、配下のモバイルI PをサポートしないC Nに代わってH AからのC Nへの結合更新メッセージを代理受信し、結合更新で通知されたV P N情報が設定されたサービスプロファイルを基に、C Nに代わってF Aへの結合トンネルをI P S e cトンネルで設定するプロトコル処理を行なう。

【 0 0 2 3 】

移動端末（M N）1のホームネットワーク3にあるネットワーク装置（H A）のM A V P N制御部は、前記トンネルの設定の際にサービスプロファイルでセキュリティ保護が要求されるとR F C 2 0 0 2で規定されたH Aから移動端末の現

在の接続点である外部ネットワーク2にあるネットワーク装置（FA）に設定するトンネルを通常のIP-IPトンネルに代わりIPSecトンネルを設定し、一方FAの側のMAVPN制御部もサービスプロファイルでセキュリティ保護が要求されると、FAからHAへのトンネル（通常リバーストンネルと呼ばれる）をIP-IPトンネルではなくIPSecトンネルで設定する。

【0024】

上述したように、本発明によればモバイルIPにおける位置登録手順と連携して、通信に関与する端末の公衆IPネットワークへのセキュリティゲートウェイに動的にIPSecを用いたVPNが設定される。従って、移動端末（MN）や通信先ホスト（CN）にVPN用の特殊な機能を持たせることなく任意の端末やホスト間でVPN設定サービスが提供可能となる。また、ネットワーク側でVPN設定サービスが提供されるため、ユーザによる自由な組み合わせによるサービス品質、セキュリティレベル、及び経路等の指定が可能となる。

【0025】

【発明の実施の形態】

図4は、本発明の第1の実施例を示したものである。

本例は、初期位置登録時のVPN設定例（静的HA-CN間VPN存在時）を示しており、あるユーザがVPNサービスを提供しているISP（Internet Service Provider）を利用して自分が勤めている企業に公衆ネットワークからアクセスする時に、自動的にVPNが設定されるような契約をした場合を想定している。以降では、本願発明の理解の容易のため、本実施例の説明と併せて図3で示した本発明の各機能ブロックのより詳細な構成及び動作について随時説明していく。

【0026】

図4において、上記サービスを望むユーザ1は、まず企業5とホームISP3との間でVPN契約（SLA：Service Level Agreement）を取り交わす①。契約内容は使用するSPI（Security Parameter Index）と鍵群、サービス品質、このVPNを利用可能なユーザのリストである。企業側は前記SLAに基づき、自企業のVPNGW装置51にISP3のHA31のVPN情報を設定する

。ISP側は企業に示されたユーザのVPNデータベースにこの企業ドメインのアドレスとSPI、鍵等を設定する。またVPN情報35としてCN-GW対応表に企業ドメインアドレスとVPNGW装置51のアドレスを登録し、GW種別にVPN動的設定不可を設定する。

【0027】

図5には、本発明で使用するVPNデータベースの構成例を示している。

VPNデータベース34は各ユーザの設定したVPNデータインスタンス1～nの集合であり、各インスタンスが一つのVPNに対応する。各VPNデータインスタンスは、このVPN情報を一意に表す識別子であるプロフィール番号(Profile Number)、ユーザのネットワーク識別子(NAI; Network Access Identifier)、セキュリティゲートウェイ間の共有のセキュリティ関係を使用するか又はユーザ固有のセキュリティ関係を使用するかを示すVPN共有指標(vpnshare)、通信先端末のIPアドレス(destaddr)、上り方向のQoSクラス(upclass)、下り方向のQoSクラス(downclass)、IPSecで使用する上り方向SPI(upSPI)、IPSecで使用する下り方向SPI(downSPI)で構成される。

【0028】

前記VPN共有指標に0が設定された場合、upclass, downclass, upSPI, downSPIは省略可能である。このデータベースはユーザのNAIで検索され、検索された全てのインスタンスは後述するVPN情報キャッシュにアドレス情報を付加して記録される。なお、データ検索に使用するデータベース検索プロトコルはVPNデータベースを実装するデータベースの製品等に依存しており、通常はLDAP(Light Directory Access Protocol)やSQLが用いられる。また、上述したVPN情報35のCN-GW対応表については後述の図8にその一例を示す。

【0029】

次に、ユーザ1は企業が契約を交わしたホームISP3とローミング契約をしているISP2の任意のアクセスポイントに接続し、モバイルIPの位置登録要求(Reg Req)(②)を送出することでネットワークの利用が可能になる

。ローミング契約しているISP2の接続ポイントとなるFA21はこの登録要求を認証要求メッセージ(AMR) (③) に含めて、自ISP内のローカルAAAサーバ(AAAF) 23を介して、ユーザのホームISP3のAAA(AAAH) 33に送出する。

【0030】

AAAHは認証要求メッセージ(AMR) に含まれるNAIでVPNデータベース34を検索し、このユーザに固有のVPN情報35を抽出する。また、そのCN-GWアドレス対応表よりVPNデータベースで通信先として指定されている企業ドメインのアドレスはVPN動的設定不可であることがわかるので、後述するVPN情報キャッシュにFA-HA, HA-企業GWの2つのVPNを設定する。次に、HAに対してこの2つのVPNのプロファイルを付加した位置登録要求メッセージ(HAR) を送信する(④)。

【0031】

図6にはAAAの詳細機能ブロックを、そして図7～12にはその動作例を示している。

図6において、AAA33(23も同様)は、図3で示したAAAプロトコル制御部301、AAAVPN制御部302に加えて、アプリケーションサーバ305、ネットワークカーネル303、及び物理ネットワークデバイスインタフェース304から構成される。AAAプロトコル制御部302は、AAAプロトコルを制御するAAAプロトコル処理部311から構成される。

【0032】

AAAVPN制御部302は、VPNデータベース(図5)より抽出したVPN情報をキャッシュするVPN情報キャッシュ312、VPN経路決定制御部313、鍵生成器315から構成される。図7には、VPN情報キャッシュ312の一例を示している。VPN情報キャッシュ312はVPN情報キャッシュインスタンス1～nの集まりであり、ユーザがネットワークにアクセスしている間有効なネットワークで一意的なユーザに固有な情報を含むセッションIDで検索される。各VPN情報キャッシュインスタンス1～nは一意的な識別子であるセッションID、このユーザが設定しているVPNの数を示すプロファイル数、各VPN

の設定情報を含むVPN情報プロファイル1～nで構成される。

【0033】

各VPN情報プロファイル1～nは、VPNを一意に識別する識別子であるプロファイル番号、VPN適用のパケットを特定するための送信元と宛先のIPアドレスとそのネットマスク、パケットに設定するTOS値、IPSecをAH、ESP、カプセル化のみ、のいずれかで設定するかを示すセキュリティタイプ、IPSecトンネルモードで参照されるIPSecトンネルの入口と出口である送信元と宛先のゲートウェイアドレス、宛先ゲートウェイが動的なVPN設定が可能かどうかを示す宛先GW種別、上りと下り方向のセキュリティ関係の識別子であるSPI (Security Parameter Index)、ESP暗号鍵、ESP認証鍵で構成される。

【0034】

VPN経路決定制御部313は、その内部にCN-GWアドレス対応表314を有しており、図8にCN-GWアドレス対応表の一例を示している。CN-GWアドレス対応表は、CNアドレス/ネットマスク、GWアドレス、及びGW種別を含むアドレスインスタンス1～nから構成され、CNアドレス/ネットマスク（企業ドメインアドレス）をキーとして検索される。

【0035】

アプリケーションサーバは、VPNデータベース34とWEBアプリケーション36から構成される。ネットワークカーネル303はIPパケットの回送とネットワークへの接続点である物理インタフェースを制御するオペレーティングシステムである。物理ネットワークデバイスインタフェース304は物理ネットワークデバイスへのインタフェース（ハード制御ドライバ）であり、通常はLANのNICカードである。

【0036】

図9～13は、AAAの処理フローの一例を示している。

図9はAAAの全体処理フロー例であって、ネットワークカーネル303が物理ネットワークインタフェース304からパケットを受信すると、そのポート番号によりAAAシグナリングパケットを選択し、AAAプロトコル制御部301

に受信パケットの情報を渡す（S100）。図10はAAAプロトコル処理部311の処理フロー例である。まず、受信したAAAプロトコルのコマンドコードAVP（属性パラメータ）より受信メッセージを判定する（S101）。認証要求メッセージ（AMR）であればステップS102へ、後述する認証応答メッセージ（AMA）であればステップS103へ、その他であればステップS104へ処理を分岐する。

【0037】

上記した本例の場合には、AAAVPN制御部302を起動する（S102）。次に、VPNデータベース34より抽出したVPN情報又は認証応答メッセージ（AMA）をVPN情報キャッシュに設定する（S103）。そして、CN-GW対応表に従って対応メッセージを編集、例えば、差別化サービスの設定等をしてから送出する（S104）。AAAH33が送出する認証応答メッセージ（AMA）及び位置登録要求メッセージ（HAR）にはVPN情報キャッシュを設定した旨のプロファイルキャッシュAVP（Profile Cache AVP）を設定する。なお、図11には、図10のステップS103におけるメッセージ対応表（送受信メッセージとその処理実行主体との関係）を示している。

【0038】

図12は、AAAVPN制御部302の処理フロー例である。AAAVPN制御部302は、始めにVPNデータベース34を移動端末のNAIで検索して対応するVPN情報を読み出す（S105）。次にVPN経路決定制御部313を起動し（S106）、そしてVPNデータベース34から読み出したSPI（Security Parameter Index）がデフォルトSPIであれば処理を終了し、そうでなければ鍵生成器315で個別の鍵を生成する（S108）。

【0039】

図13は、VPN経路決定制御部313の処理フロー例である。VPN経路決定制御部313は、認証要求メッセージ（AMR）の要求元ホストアドレスからMN1側のVPNGW（FA）21のアドレスを抽出する（S109）。また、VPNデータベース34から読み出したCNアドレスによりCN-GWアドレス対応表314を検索してCN52側のVPNGW51のアドレスとVPNGW種

別を読み出す（S110）。

【0040】

次に、前記VPNGW種別が動的VPN設定可能であればステップS112へ、そうでなければステップS113へ処理を分岐する（S111）。本例ではステップS113の処理を行なうことになる。この場合、HA31へ通知するVPN情報の送信元GWアドレスにHA31のアドレス、宛先GWアドレスにCN-GWアドレス対応表314から読み出したGW51のアドレスを設定する。また、FA21へ通知するVPN情報の送信元GWアドレスにFA21のアドレス、宛先GWアドレスにHA31のアドレスを設定して処理を終了する（経路をFA-HA-CNに設定）。

【0041】

一方、VPNGW種別が動的VPN設定可能であれば、HA31へ通知するVPN情報の宛先GWアドレスにFA21のアドレス、送信元GWアドレスにCN-GWアドレス対応表314から読み出したGW51のアドレスを設定する。FA21へ通知するVPN情報の送信元GWアドレスにFA21のアドレス、宛先GWアドレスに同じくCN-GWアドレス対応表より読み出したGW51のアドレスを設定し終了する（経路をFA-CN（又はPCN）に設定）。

【0042】

図4に戻って、次にHA31はAAAH33から受信した位置登録要求メッセージ（HAR）に付加されたVPN情報をキャッシュし、さらに指定された差別化サービスのマッピングを行った後、受信した経路情報に従ってHA31から企業GW51へのIPSecトンネル（2）とHA31からFA21へのIPSecトンネル（3）を設定する。また逆方向トンネルのパケットを復号するための情報を後述するIPSec情報テーブルに設定する。なお、企業側のGW51からHA31へのIPSecトンネル（1）は最初の契約設定（SLA）に基いて既に固定的に張られているため、HA31から企業GW51への設定処理は不要である。HA31は位置登録処理終了後に位置登録応答メッセージ（HAA）をAAAH33に返送する（⑤）。

【0043】

AAAH33は前記位置登録応答メッセージ(HAA)を受信すると、次にVPN情報キャッシュ312からFA-HA間のVPNを抽出し(図13のS113参照)、FA21に対して設定するこのVPNのプロファイルを付加した認証応答メッセージ(AMA)をAAAF23へ送信する(⑥)。AAAF23はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF23内にキャッシュした後にそれをFA21に回送する(図10のS101、103、及び104参照)。

【0044】

FA21は、認証応答メッセージ(AMA)に付加されたVPN情報をキャッシュし、さらに指定された差別化サービスのマッピングを行った後に、FA21からHA31へのIPSecトンネル(4)を設定する。また逆方向トンネルの packets を復号するための情報をIPSec情報テーブルに設定する。最後に、登録応答メッセージ(Reg Rep)をMN1に返送する(⑦)。その結果、MN1のアクセスポイントから企業のGW51までのVPNが設定される。なお、企業が指定していないユーザはIPSecトンネルを介してパケットが回送されないなので、これを利用して不正ユーザのアクセスを防ぐことも可能になり、また複数のISPとSLAを契約する煩わしさから逃れることができる。

【0045】

図14にはMA(FA、HA、PCN)の詳細機能ブロックを、そして図15～24にはその動作例を示している。

図14において、FA、HA、PCNの各ネットワーク装置は、MAプロトコル制御部321、MAVPN制御部322、ネットワークカーネル323、及び物理ネットワークデバイスインタフェース324から構成される。MAプロトコル制御部321は、AAAプロトコルを制御するAAAプロトコル処理部331とモバイルIPを制御するモバイルIPプロトコル処理部332から構成される。また、MAVPN制御部322は、AAA又はMIPプロトコルにより通知されたVPN情報をキャッシュするVPN情報キャッシュ333、QoS制御部334、及びトンネル制御部335から構成される。

【0046】

VPN情報キャッシュ333は先に図7で説明したのと同様の構成である。QoS制御部334は、VPN情報キャッシュ333に設定されたTOS値と、TOS値をマーキングするパケットを識別するための送信元アドレス、宛先アドレス及びそれらのネットマスクからなるフィルタ情報をネットワークカーネル323に設定する。トンネル制御部335は、VPN情報キャッシュ333に設定された宛先のIPアドレスに対してルートテーブル337の出口デバイスを仮想デバイスに書き換える。またIPSec情報テーブル336に送信元と宛先のIPアドレスとそのネットマスク、セキュリティタイプ、送信元と宛先のゲートウェイアドレス、上りと下り方向のセキュリティ関係の識別子であるSPI、ESP暗号鍵、ESP認証鍵を設定する。ネットワークカーネル323から仮想デバイスに出力されたパケットはIPSec情報テーブル335を参照して、暗号化とカプセル化が実行される。

【0047】

図15には、IPSec情報テーブル333の一例を示している。IPSec情報テーブルは、IPSec情報、ESP情報、トンネル情報で構成される。IPSec情報はIPSec情報インスタンスの集まりであり、送信元アドレスと宛先アドレスの組で特定される。IPSec情報インスタンスは送信元アドレス／ネットマスク、宛先アドレス／ネットマスク、パケットの実際の回送先である実宛先アドレス、このパケットに適用するトンネル情報の識別子、このパケットに適用するESP情報の識別子から構成される。ESP情報はESP情報インスタンスの集まりであり、ESP情報を一意に識別するESP識別子、暗号化手法、方向、AH認証鍵長、ESP認証鍵長、ESP暗号鍵長、AH認証鍵、ESP認証鍵、ESP暗号鍵で構成される。トンネル情報はトンネル情報インスタンスの集まりであり、トンネル情報を一意に識別するトンネル識別子、カプセル化手法、方向、トンネルの入口と出口になる送信元アドレスと宛先アドレスから構成される。

【0048】

ネットワークカーネル323は、IPパケットの回送とネットワークへの接続点である物理インタフェースを制御するオペレーティングシステムであり、IP

パケット回送のルートを決めるルーティングテーブル 3 3 7 を持つ。ネットワークカーネル 3 2 3 は IP パケットのカプセル化、パケット編集、パケット送出のキュー制御等を行うが、これらの機能はオペレーティングシステムに依存しており、本発明では言及しない。

【 0 0 4 9 】

図 1 6 にルーティングテーブル 3 3 7 の一例を示す。一般的なルーティングテーブル 3 3 7 は、宛先アドレス、ゲートウェイアドレス、ネットマスク、メトリック、出口インタフェースとその他の制御用補助情報から構成されており、宛先アドレスとメトリックでルートが決定される。本発明はルートテーブルの構成には依存しないが、出力先に仮想デバイスを設定できるようなネットワークカーネルを例に以降の具体的な説明を行う。又、ネットワークカーネルはカプセル化されたパケットを受信すると、パケットをデカプセル化する機能を持っており、デカプセル後のパケットが ESP ヘッダを含んでいれば、トンネル制御部 3 3 5 で保持している ESP 情報を参照して暗号化されたパケットをデコードする機能を持つ。物理ネットワークデバイスインタフェース 3 2 4 は物理ネットワークデバイスへのインタフェース（ハード制御ドライバ）であり、物理ネットワークデバイスは例えば LAN, ISDN, ATM 等のパッケージ又は NIC カードである。

【 0 0 5 0 】

図 1 7 ～ 2 4 には、MA の処理フロー例を示している。以下、各処理フロー例を用いて本願発明による MA 処理について説明する。

図 1 7 は、MA の全体処理フローである。ネットワークカーネル 3 2 3 は物理ネットワークインタフェース 3 2 4 よりパケットを受信すると、既に概略を説明したようにデカプセル化及び暗号化復号を行った後、受信パケットをシグナリングパケットかデータパケットかで切り分ける（S 2 0 0）。シグナリングパケットの選択は MA プロトコル制御部 3 2 1 が指定したポート番号でパケットを受信したかどうかで決定される。シグナリングパケットであればステップ S 2 0 1、それ以外であればステップ S 2 0 3 へ処理を分岐する。

【 0 0 5 1 】

シグナリング packets の場合は MA プロトコル制御部 321 へ受信 packets の情報を渡し、AAA プロトコル処理 331 及びモバイル IP プロトコル処理 332 を行う (S201)。次に、MA VPN 制御部 322 を起動して VPN 情報の設定を行う (S202)。ステップ S203 では、ネットワークカーネルが受信 packets の出力先のインタフェースを、ルーティングテーブル 337 を参照して決定する。ネットワークカーネル 323 はカーネル内に予め設定された差別化サービスのフィルタリング条件に従って packets の編集を行う。出力先が仮想デバイスであればステップ S204 へ処理を分岐する。出力先が物理デバイスであれば、そのデバイスへ packets を回送する。

【0052】

ステップ S204 では、MA VPN 制御部 322 へ回送する packets の情報を渡し、予め設定された情報に基づきトンネル化及び暗号化処理を行う。トンネル処理で IP packets をカプセル化する場合は、オリジナル packets の TOS 情報を引き継ぐ。IP packets の編集が終了した packets は、再度、ネットワークカーネル 323 に戻され、新しく付与された IP packets の宛先に基づいてルーティングテーブル 337 が参照されて対応する物理デバイスへ packets の回送が行われる。

【0053】

図 18 は、MA プロトコル制御部 321 の処理フロー例である。先ず、受信した packets のポート番号を調べ、AAA プロトコルのポート番号であればステップ S206 へ、一方モバイル IP プロトコルであればステップ S207 へ処理を分岐する (S205)。ステップ S206 では、AAA プロトコル処理部 331 を起動して AAA プロトコルの処理後に (図 19 参照)、AAA プロトコルに情報の一部として付加されているモバイル IP プロトコルを取り出してステップ S207 へ処理を渡す。ステップ S207 では、モバイル IP プロトコル処理部 332 を起動して処理を終了する。

【0054】

図 19 は、AAA プロトコル処理部 331 の処理フロー例である。先ず、受信した AAA プロトコルより、VPN 情報を抽出してそれを VPN 情報キャッシュ

3 3 3 へ設定する。次に、後述のモバイル I P プロトコル処理部 3 3 2 が参照するために、キャッシュの設定及び更新を行った場合に共有メモリ上に更新したことを示すフラグを立てる (S 2 0 8)。A A A プロトコルの処理後、A A A プロトコルに情報の一部として付加されているモバイル I P プロトコルを取り出す (S 2 0 9)。そして、受信メッセージが位置登録要求メッセージ (H A R) なら位置登録応答メッセージ (H A A) を送出する (S 2 1 0 及び 2 1 1)。

【 0 0 5 5 】

図 2 0 はモバイル I P プロトコル処理部 3 3 2 の処理フロー例である。ステップ S 2 1 2 では、受信したモバイル I P プロトコルメッセージのタイプを判定する。タイプが登録要求であればステップ S 2 1 3 へ、登録応答であればステップ S 2 2 0 へ、B U (Binding Update), B A (Binding Acknowledge) であればステップ S 2 1 8 へそれぞれ処理を分岐する。

【 0 0 5 6 】

A. 登録要求の場合

登録要求を受信した M A が H A の場合は、登録要求メッセージの気付アドレスと移動性結合内の旧気付アドレスとを比較し、比較結果が異なればステップ S 2 1 4 へ処理を分岐する。比較結果が一致した場合又は登録要求を受信した M A が F A の場合はステップ S 2 1 7 へ処理を分岐する (S 2 1 3)。ステップ S 2 1 4 では位置登録メッセージを送出した M N の V P N 情報キャッシュインスタンスを特定し、V P N 情報キャッシュ 3 3 3 の宛先 G W アドレスを気付アドレスで通知されたアドレスに書き換える。

【 0 0 5 7 】

この特定方法は例えばセッション I D に M N の I P アドレスを持たせることや、移動性結合と V P N 情報キャッシュインスタンスのリンクを持たせることで実現可能である。H A は特定した V P N 情報キャッシュインスタンスに設定されている全ての V P N 情報プロファイルを検索し、宛先 G W 種別が動的 V P N 設定可能であれば、そのプロファイルの送信元アドレスに対して V P N 情報を設定した B U メッセージを編集して送出する (S 2 1 5)。ステップ S 2 1 6 では M A V P N 制御部 3 2 2 を起動し、図 2 1 のメッセージ対応表に示すように、受信メッ

ページと処理MAで特定されるメッセージを編集して送出する（S 2 1 7）。

【0 0 5 8】

B. 登録応答の場合

ステップS 2 2 0では、AAAプロトコル処理部3 3 1によりあらかじめ共有メモリに設定されたキャッシュ更新情報を参照し、更新有りであればステップS 2 1 6へ、更新無しであればステップS 2 1 7へ処理を分岐する。

【0 0 5 9】

C. BU, BAの場合

ステップS 2 1 8では、受信メッセージがBUであればステップS 2 1 9へ、BAであればステップS 2 1 7へ処理を分岐する。PCNの場合は、PCN配下のCN宛てのBUメッセージを全て代理受信する。この仕組みは、例えば特許2 0 0 0 - 3 2 3 7 2の方式で実現される。処理MAがPCNの場合はBUメッセージに設定されたVPN情報をVPN情報キャッシュ3 3 3に設定もしくは置換する。処理MAがFAの場合はVPN情報キャッシュ3 3 3の宛先GWアドレスをBUメッセージで通知された新FAアドレスに変更する（S 2 1 9）。

【0 0 6 0】

図2 2は、MA VPN制御部3 2 2の処理フロー例である。ステップS 2 2 1ではQoS制御部3 3 4を起動し、次にステップS 2 2 2でトンネル制御部3 3 5を起動する。

図2 3は、QoS制御部3 3 4の処理フロー例である。まず、ステップS 2 2 3でVPN情報インスタンスの情報を元にネットワークカーネル3 2 3に設定済みの差別化サービスの情報を削除する。次に、VPN情報インスタンスのTOS値が0以外であればステップS 2 2 5へ処理を分岐し、そうでなければ処理を終了する（S 2 2 4）。ステップS 2 2 5では、VPN情報インスタンスの情報を元にネットワークカーネルに差別化サービスの情報を設定する（S 2 2 5）。

【0 0 6 1】

図2 4は、トンネル制御部の処理フロー例である。まず、VPN情報インスタンスの情報を元にネットワークカーネル3 2 3に設定済みのルートテーブル3 3 7の情報とIPSec情報テーブル3 3 6の該当する情報を削除する（S 2 2 6

）。次に、VPN情報インスタンスのVPN情報プロファイルに設定された宛先アドレスの出力先を仮想デバイスに設定し（S 2 2 7）、またVPN情報インスタンスのVPN情報プロファイルを参照して、IPSec情報テーブル336のトンネル情報インスタンスを設定する（S 2 2 8）。

【0062】

ステップS 2 2 9では、VPN情報インスタンスのVPN情報プロファイル内セキュリティタイプを参照して、ESPかAHが指定されていればステップS 2 3 0へ処理を分岐し、そうでなければ処理を終了する。ステップS 2 3 0では、VPN情報インスタンスのVPN情報プロファイル内SPIを参照して、SPIがユーザ個別であればステップS 2 3 1へ、デフォルトSPIであればステップS 2 3 2へ処理を分岐する。このデフォルトSPIについては予めMA内に初期構成時やMAのローカルな保守コンソールから設定されているものとする。ステップS 2 3 1では、VPN情報インスタンスのVPN情報プロファイルのSPIと関連する鍵情報をESP情報インスタンスに設定する。また、ステップS 2 3 2では、IPSec情報インスタンスにESP識別子を設定する。

【0063】

以降では、これまで説明してきた事項をもとに、本願発明動作の理解をより一層深めるために、先に説明した第1の実施例とは別の本発明の種々の実施態様例について説明する。

図25は、本発明の第2の実施例を示したものである。

本例は、同一ドメイン内移動時のVPN設定例（静的HA-CN間VPN存在時）を示している。ここでは、先の実施例1でローミング契約ISP2のFA21から企業ドメインのGW51にVPNが設定された後、ユーザのMN1が同一ローミング契約ISP2の別のFA21'に移動した場合に、どのようにVPNが再構築されるかを図式的に示している。

【0064】

図25において、ユーザのMN1が同一ドメイン2内でFA21から新FA21'へ移動すると、モバイルIP経路最適化ドラフト（draft-ietf-mobileip-opt-09）に規定されているように、旧FA21のアドレスを含めた登録要求メッ

セージ (Reg Req) を送出する (①)。新FA21' はこの登録要求を認証要求メッセージ (AMR) に含めて (②)、自ISP2内のローカルAAAサーバ (AAAF) 23に送出する。AAAF23は、認証要求メッセージ (AMR) に旧FA21の情報が含まれている場合、VPN情報キャッシュからFA-HAのVPNを抽出してFA21のアドレスを新FA21' のアドレスに置換した後、FAに設定するこのVPNのプロファイルを付加した認証応答メッセージ (AMA) を新FA21' へ返送する (③)。

【0065】

FA21' は先にMN1から受信した登録要求メッセージ (Reg Req) をHA31に回送する (④)。HA31はVPN情報キャッシュのうち、HAからFAへのVPNプロファイルを特定し、FAのアドレスを新FA21' に書き換える。次に、旧FA21へのIPSecトンネルを削除し、新FA21' へ新たなIPSecトンネル (1) を設定する。そして、位置登録処理終了後、登録応答メッセージ (Reg Rep) をFA21' に返送する (⑤)。

【0066】

FA21' は、VPN情報キャッシュを参照して指定された差別化サービスのマッピングを行った後、FA21' からHA31へのIPSecトンネル (2) を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。さらに、VPN情報キャッシュを複写して送信元GWアドレスを旧FA21、宛先GWアドレスを新FA21' に書き換えた後に、このVPN情報をBUメッセージに付加して旧FA21に送信する (⑥)。

【0067】

旧FA21はBUメッセージに付加されたVPN情報をキャッシュし、FA21からHA31へのIPSecトンネルを削除し、指定された差別化サービスのマッピングを行った後、旧FA21から新FA21' へスムースハンドオフ時のIPSecトンネル (3) を設定する。その結果、HA31が新たなIPSecトンネル (1) への切り替え前にMN1宛に旧FA21で受信したパケットは全てこのIPSecトンネル (3) を介して新FA21' へ回送される。旧FA21はIPSecトンネル (3) の設定完了後にBAメッセージをMNに返送する

(⑦)。これにより、新FA21'は登録応答メッセージ(Reg Rep)をMN1に返送する(⑧)。

【0068】

図26は、本発明の第3の実施例を示したものである。

本実施例は、異なる管理ドメイン間移動時のVPN設定例(静的HA-CN間VPN存在時)を示しており、ここでは、実施例1でローミング契約ISP2のFA21から企業ドメインのGW51にVPNが設定された後、ユーザのMN1が異なるローミング契約ISP2'の別のFA21'に移動した場合に、どのようにVPNが再構築されるかを図式的に示している。

【0069】

図26において、ユーザのMN1は異なる管理ドメイン2-2'間を移動すると、DIAMETERモバイルIP拡張ドラフト(draft-ietf-calhoun-diameter-mobileip-08)に規定されているように、通常の初回位置登録と同じ手順で、登録要求(Reg Req)を送出する(①)。移動先のFA21'はこの登録要求を認証要求メッセージ(AMR)に含め(②)、自ISP内のローカルAAAサーバ(AAAF)22'を介して、ユーザのホームISPのAAA(AAAH)33に送出する。

【0070】

AAAH33は、VPN情報キャッシュにFA-HA、HA-企業GWの2つのVPNが設定済なので、FA-HAに関するVPNのFAを新FA21'のアドレスに書き換える。次に、HA31にこの2つのVPNのプロファイルを付加した位置登録要求メッセージ(HAR)を送信する(③)。HA31は、位置登録要求メッセージ(HAR)に付加されたVPN情報でキャッシュを更新し、HA31から旧FA21へのIPSecトンネルを削除後、新FA21'への新たなIPSecトンネル(1)を設定する。そして、位置登録処理終了後、位置登録応答メッセージ(HAA)をAAAHに返す(④)。この時、旧FA21のアドレスの情報を付加情報として返す。

【0071】

AAAH33は位置登録応答メッセージ(HAA)を受信すると、VPN情報

キャッシュからFA-HAのVPNを抽出し、FAに設定するこのVPNのプロファイルを付加した認証応答メッセージ(AMA)をAAAF23'へ送信する(⑤)。AAAF23'はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF内にキャッシュした後、それをFA21'に回送する。FA21'は、認証応答メッセージ(AMA)に付加されたVPN情報をキャッシュし、指定された差別化サービスのマッピングを行った後にFA21'からHA31へのIPSecトンネル(2)を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。

【0072】

さらに、認証応答メッセージ(AMA)に旧FAのアドレスが含まれている場合はVPN情報キャッシュを複写し、送信元GWアドレスを旧FA21、宛先GWアドレスを新FA21'に書き換えた後にこのVPN情報をBUメッセージに付加して旧FA21に送信する(⑥)。旧FA21はBUメッセージに付加されたVPN情報をキャッシュし、FAからHAへのIPSecトンネルを削除し、指定された差別化サービスのマッピングを行った後にこのFA21から新FA21'へハンドオフ時のIPSecトンネル(3)を設定する。

【0073】

その結果、HA31がIPSecトンネル(1)への切り替え前にMN1宛に旧FA21が受信したパケットは全てこのIPSecトンネル(3)を介して新FA21'へ回送される。FA21はIPSecトンネル(3)の設定完了後にBAメッセージを新FA21'に返す(⑦)。これにより、FA21'は登録応答メッセージ(Reg Rep)をMN1に返送する(⑧)。

上述した実施例2及び3によれば、企業とISPを介して通信を行うユーザは、企業のGW装置に特殊な機能を持つことなく、ISPが提供するモバイル対応VPNのサービスを享受する事が可能となる。

【0074】

図27は、本発明の第4の実施例を示したものである。

本実施例は、初期位置登録時のVPN設定例(PCN存在時)を示しており、ここでは通信先のローミング契約ISPが動的にVPN設定可能なVPN GW

(PCN) を配備している場合のVPN設定例を図式的に示している。動的にVPN設定可能なVPNGWを持つISPはISP間でローミング契約を結ぶときに、各々のプロバイダのCN-GW対応表にISPのドメインアドレスとGW装置アドレスを登録し、GW種別にVPN動的設定可を設定する。

【0075】

図27において、これらのローミンググループのいずれかのISPに加入しているユーザは最寄りのアクセスポイントに接続し、そのMN1よりモバイルIPの位置登録要求(Reg Req)を送出する(①)。FA21はこの登録要求を認証要求メッセージ(AMR)に含めて自ISP内のローカルAAAサーバ(AAAF)23を介して、ユーザのホームISPのAAA(AAAH)33に送出する(②)。

【0076】

AAAH33は、認証要求メッセージ(AMR)に含まれたNAIでVPNデータベース34を検索し、このユーザに固有のVPN情報を抽出する。VPNデータベース34にユーザ通信先として指定しているアドレスがローミング契約ISP4内であれば、CN-GWアドレス対応表からVPN動的設定可であることがわかるので、VPN情報キャッシュにFA-通信先ISP4のGW(PCN)41のVPNを設定する。HA31にこのVPNのプロファイルを付加した位置登録要求メッセージ(HAR)を送信する(③)。HA31は位置登録要求メッセージ(HAR)に付加されたVPN情報をキャッシュする。そして、位置登録処理終了後、VPN情報に設定された通信先GW41のGW種別を参照し、VPN動的設定可であるので、通信先端末CN42宛てにこのVPN情報を付加したMIP結合更新メッセージBUを送出する(④)。

【0077】

PCN41は、CN42宛てに送出されたBUを代理受信し、BUに付加されたVPN情報をキャッシュする。通知されたVPN情報に従い差別化サービスのマッピングを行った後、PCN41からFA21へIPSecトンネル(1)を設定する。その後、MIP結合承認メッセージBAをHA31に送出する(⑤)。HA31はBAを受信すると位置登録応答メッセージ(HAA)をAAAH33

3に返す(⑥)。AAA H 3 3は位置登録応答メッセージ(HAA)を受信すると、VPN情報キャッシュからFA-通信先ISP 4のGW(PCN)のVPNを抽出し、FA 2 1に設定するこのVPNのプロファイルを付加した認証応答メッセージ(AMA)をAAAF 2 3へ送信する(⑦)。AAAF 2 3はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF内にキャッシュした後、FA 2 1に回送する。

【0078】

FA 2 1は認証応答メッセージ(AMA)に付加されたVPN情報をキャッシュし、指定された差別化サービスのマッピングを行った後、FA 2 1からPCN 4 1へIPSecトンネル(2)を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。その後、登録応答メッセージ(Reg Rep)をMNに返す(⑧)。これにより、ローミング契約をしたISPグループ内であれば、ユーザは任意の通信先とVPN通信をすることができる。

【0079】

図28は、本発明の第5の実施例を示したものである。

本実施例は、同一ドメイン内移動時のVPN設定例(PCN存在時)を示しており、ここでは実施例4でローミング契約ISP 2のFA 2 1から任意のローミング契約ISP 4のPCN 4 1にVPNが設定された後、ユーザのMN1が同一ローミング契約ISP 2の別のFA 2 1'に移動した場合に、どのようにVPNが再構築されるかを図式的に示している。

【0080】

図28において、ユーザのMN1は同一ドメイン2内でFA 2 1からFA 2 1'へ移動すると、モバイルIP経路最適化ドラフト(draft-ietf-mobileip-opti m-09)に規定されているように、登録要求メッセージ(Reg Req)には旧FA 2 1のアドレスを含めて送出する(①)。新FA 2 1'はこの登録要求を認証要求メッセージ(AMR)に含めて自ISP内のローカルAAAサーバ(AAA F) 2 3に送出する(②)。AAAF 2 3は、認証要求メッセージ(AMR)に旧FA 2 1の情報が含まれている場合、VPN情報キャッシュからFA-PC

NのVPNを抽出し、FAのアドレスを新FA21'のアドレスに置換した後、FAに設定するこのVPNのプロファイルを付加した認証応答メッセージ（AM A）を新FA21'へ送信する（③）。

【0081】

FA21'は先にMN1から受信した登録要求メッセージ（Reg Req）をHA31に回送する（④）。HA31はVPN情報キャッシュのうち、このMN1が利用しているVPNのVPNプロファイルを特定し、FAのアドレスを新FA21'に書き換える。本実施例の場合、既にVPNはFA21とPCN41との間に直接設定されているため、その旨をPCN41へBUメッセージで通知する（⑤）。なお、BUメッセージを送出するか否かはVPN情報キャッシュの通信先GWの種別が動的VPN設定可であるかどうかで判定する。

【0082】

PCN41は、BUの受信により旧FA21へのIPSecトンネルを削除し、それに代えて新FA21'へのIPSecトンネル（1）を設定する。その後、BAメッセージをHA31に送信する（⑥）。HA31はBAメッセージの受信により登録応答メッセージ（Reg Rep）を新FA21'に送信する（⑦）。新FA21'はVPN情報キャッシュを参照して、指定された差別化サービスのマッピングを行った後、新FA21'からPCN41へIPSecトンネル（2）を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。更にVPN情報キャッシュを複写し、送信元GWアドレスを旧FA21、宛先GWアドレスを新FA21'に書き換えた後、このVPN情報をBUメッセージに付加して旧FA21に送信する（⑧）。

【0083】

旧FA21はBUメッセージに付加されたVPN情報をキャッシュし、旧FA21からPCN41へのIPSecトンネルを削除し、指定された差別化サービスのマッピングを行った後に旧FA21から新FA21'へスムーズハンドオフ時のIPSecトンネル（3）を設定する。旧FA21がIPSecトンネルへの切り替え前にPCN41からMN1宛に受信したパケットは全てこのIPSecトンネル（3）を介して新FA21へ回送される。FA21は、IPSecト

ンネル設定完了後にBAメッセージを返送する(⑨)。新FA21'は登録応答メッセージ(Reg Rep)をMN1に返送する(⑨')。

【0084】

図29は、本発明の第6の実施例を示したものである。

本実施例は、異なる管理ドメイン間移動時のVPN設定例(PCN存在時)を示しており、ここでは実施例4でローミング契約ISP2のFA21から任意のローミング契約ISP4のPCN41にVPNが設定された後、ユーザのMN1が異なるローミング契約ISP2'の別のFA21'に移動した場合に、どのようにVPNが再構築されるかを図式的に示している。

【0085】

図29において、ユーザのMN1は異なる管理ドメイン間2-2'を移動すると、DIAMETERモバイルIP拡張ドラフト(draft-ietf-calhoun-diameter-mobileip-08)に規定されているように、通常の初回位置登録と同じ手順で登録要求メッセージ(Reg Req)を送出する(①)。FA21'はこの登録要求を認証要求メッセージ(AMR)に含めて自ISP内のローカルAAAサーバ(AAAF)23'を介して、ユーザのホームISPのAAA(AAAH)33に送出する(②)。AAAH33は、VPN情報キャッシュにFA21-PCN41のVPNが設定済なので、このFA21のアドレスを新FA21'のアドレスに書き換える。そして、HA31にはこのVPNのプロファイルを付加した位置登録要求メッセージ(HAR)を送信する(③)。

【0086】

HA31は、位置登録要求メッセージ(HAR)に付加されたVPN情報でキャッシュを更新し、BUメッセージをPCN41へ送出する(④)。PCN41はBUメッセージを受信すると、旧FA21へのIPSecトンネルを削除し、新FA21'へIPSecトンネル(1)を設定する。その後、BAメッセージをHA31に送信する(⑤)。HA31はBAメッセージを受信すると位置登録応答メッセージ(HAA)をAAAH33に返送する(⑥)。この時、旧FA21のアドレスの情報を付加情報として返す。

【0087】

AAAH33は位置登録応答メッセージ(HAA)を受信すると、VPN情報キャッシュからFA-PCNのVPNを抽出し、FAに設定するこのVPNのプロファイルを付加した認証応答メッセージ(AMA)をAAAF23'へ送信する(⑦)。AAAF23'はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF内にキャッシュした後、それを新FA21'に回送する。新FA21'は認証応答メッセージ(AMA)に付加されたVPN情報をキャッシュし、指定された差別化サービスのマッピングを行った後、新FA21'からPCN41へのIPSecトンネル(2)を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。

【0088】

本例のように認証応答メッセージ(AMA)に旧FA21のアドレスが含まれている場合は、VPN情報キャッシュを複製し、送信元GWアドレスを旧FA21、宛先GWアドレスを新FA21'に書き換えた後、このVPN情報をBUメッセージに付加して旧FA21に送信する(⑧)。旧FA21はBUメッセージに付加されたVPN情報をキャッシュし、旧FA21からPCN41へのIPSecトンネルを削除し、指定された差別化サービスのマッピングを行った後、このFA21から新FA21'へスムーズハンドオフ時のIPSecトンネル(3)を設定する。

【0089】

IPSecトンネルの切り替え前にMN1宛にPCN41から受信したパケットは全てこのIPSecトンネルを介して新FA21'へ回送される。旧FA21はIPSecトンネル(3)の設定完了後にBAメッセージをMNに返す(⑨)。それにより、新FA21'は登録応答メッセージ(Reg Rep)をMN1に返送する(⑨')。実施例5及び6に示すように、本発明によればローミング契約ISPグループに加入しているユーザはグループ内の任意の通信先とVPNを設定でき、またVPNを保持したままでグループ内を自由に移動することができる。

【0090】

図30は、本発明の第7の実施例を示したものである。

本実施例はユーザ指定の任意の端末間でのVPN設定例を示しており、これまではユーザが指定した特定の通信先に対してVPNを設定する例を示したが、ユーザがVPNを設定する通信先を動的に設定することもできる。この実施例では、ユーザが契約時に指定していた通信先以外の通信先にVPNを設定する例を示す。

【0091】

VPN設定先の変更を望むユーザは、ユーザのホームISP3が提供するVPNサービスカスタマイズ用のホームページにアクセスする。ユーザは、このホームページを介して、通信先のアドレスを設定する。このホームページと連動したWEBアプリ36はVPNデータベース34の該ユーザのVPN情報をユーザが指定した情報に変更する(①)。ユーザのMN1はカスタマイズが終了すると、サービス更新要求を付加した位置登録要求メッセージ(Reg Req)を現在接続しているFA21へ送出する(②)。FA21はサービス更新要求が付加された登録要求を受信すると、この登録要求を認証要求メッセージ(AMR)に含めて自ISP内のローカルAAAサーバ(AAA F)23を介して、ユーザのホームISPのAAA(AAA H)33に送出する(③)。

【0092】

AAAH33は、VPN情報キャッシュが既に存在するか否かに関係なくサービス更新要求が付加されたメッセージを受信すると、認証要求メッセージ(AMR)に含まれたNAIでVPNデータベース34を検索し、このユーザに固有のVPN情報を抽出する。VPNデータベース34にユーザ通信先として指定しているアドレスがローミング契約ISP内であれば、CN-GWアドレス対応表からVPN動的設定可であることがわかるので、本例ではVPN情報キャッシュにFA21-通信先ISPのGW(PCN)41'のVPNを設定する。HA31にこのVPNのプロファイルを付加した位置登録要求メッセージ(HAR)を送信する(④)。

【0093】

HA31は、位置登録要求メッセージ(HAR)に付加されたVPN情報をキャッシュする。位置登録処理終了後、VPN情報に設定された通信先GW41'

のGW種別を参照し、VPN動的設定可であるので通信先端末CN42'宛てにこのVPN情報を付加したMIP結合更新メッセージBUを送出する(⑤)。⑥

PCN41'はCN42'宛てに送出されたBUを代理受信し、BUメッセージに付加されたVPN情報をキャッシュする。通知されたVPN情報に従い差別化サービスのマッピングを行った後、PCN41'からFA21へのIPSecトンネル(1)を設定する。その後、MIP結合承認メッセージBAをHA31に返送する。

【0094】

HA31はBAメッセージを受信すると位置登録応答メッセージ(HAA)をAAAH33に返す(⑦)。AAAH33は位置登録応答メッセージ(HAA)を受信すると、VPN情報キャッシュからFA21-通信先ISPのGW(PCN)41'のVPNを抽出し、FA21に設定するこのVPNのプロファイルを付加した認証応答メッセージ(AMA)をAAAF23へ送信する(⑧)。AAAF23はMN1のローカルドメイン内での移動に対応するためVPN情報をAAAF内にキャッシュした後、それをFA21に回送する。

【0095】

FA21は認証応答メッセージ(AMA)に付加されたVPN情報をキャッシュし、指定された差別化サービスのマッピングを行った後、FA21からPCN41'へのIPSecトンネル(2)を設定する。また逆方向トンネルのパケットを復号するための情報をIPSec情報テーブルに設定する。その後、登録応答メッセージ(Reg Rep)をMNに返す(⑨)。VPN変更前に設定されていたVPNが存在していれば、VPN情報を保持しているPCN41はライフタイムの残り時間が閾値以下になった時、このVPN情報を通知してきたHA31へ結合要求メッセージBRを送出してVPNを削除して良いか尋ねる(⑨')。

【0096】

HA31はBRメッセージを受信すると、それに設定されたMN1の情報からVPN情報キャッシュを検索し、このPCN41に関するVPNがまだキャッシュされているか調べる。キャッシュされていればBUメッセージをPCN41へ

送出する。キャッシュされていなければ何も送らない。本例では P C N 4 1 はライフタイム満了までに B U が受信されないため既存の V P N を削除する。このように、ユーザが動的に V P N 設定先を指定することもできる。本実施例では、単純に W E B を介して V P N 設定先を指定する例を示したが、本発明の本質は、モバイル環境での指定された設定先への V P N 情報の配布とその設定・解放手段であり、通信先の指定方法とそれに伴う V P N データベース 3 4 への反映手段は様々なものが可能である。例えば、携帯電話による通信先と V P N コードのダイヤルや、通信先サーバからの 1 クリック V P N 設定等の応用例が考えられる。

【 0 0 9 7 】

(付記 1) モバイル I P ネットワークにおける V P N システムは、
移動端末と、

ユーザのホームネットワークに設けられたホーム認証サーバとそれ以外の外部ネットワークに設けられた外部認証サーバと、

ホームネットワークに設けられた V P N データベースと、

ホームネットワーク、外部ネットワーク、及び所定の通信ホスト及び／又はその代理サーバの各ゲートウェイ機能を有するネットワーク装置と、

で構成され、

ホーム認証サーバは、移動端末からの位置登録要求時に認証を要求したユーザの V P N 情報を V P N データベースから抽出し、その V P N 情報を所定の位置登録メッセージ及び認証応答メッセージを用いて各ネットワーク装置に通知し、

各ネットワーク装置は、通知された V P N 情報を基にホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間にそれぞれ I P S e c による V P N パスを設定する、ことを特徴とする V P N システム。

(付記 2) 認証サーバ及びネットワーク装置は、移動端末の移動による位置登録要求と連動して認証サーバ及びネットワーク装置にキャッシュされた V P N 情報を新経路情報に更新するか、又はモバイル I P で通知される位置情報で書き換えることにより、ホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置

と所定のネットワーク装置間の各VPNパスを新たなIPSecによるVPNパスに自動更新する、付記1記載のシステム。

(付記3) さらに、外部認証サーバと外部ネットワーク装置間の所定の結合更新/承認メッセージにより、それらの間のスムーズハンドオフ時にIPSecによるVPNパスを設定する、付記2記載のシステム。

(付記4) VPNデータベースは、ユーザが所望するサービス品質、セキュリティゲートウェイ間のセキュリティ・サービス情報、及びVPNを設定する通信先ホストのIPアドレス群からなるユーザ単位のVPN情報を格納する、付記1記載のシステム。

(付記5) ホーム認証サーバは、

前記VPNデータベースのVPN情報と、自身が保有すると通信先ホストを収容する所定のネットワーク装置との対応表を用い、所定の認証要求メッセージに設定された移動端末が接続した外部ネットワーク装置の情報と移動端末のホームネットワーク装置の情報からVPN設定経路を特定するAAAVPN制御部と、

各ネットワーク装置間のサービス品質とセキュリティ情報をサービスプロファイルとして、アクセスネットワークへの所定の認証応答メッセージ及びホームネットワークへの位置登録メッセージに設定するAAAプロトコル処理部と、

を有する付記1記載の装置。

(付記6) 各ネットワーク装置は、

キャッシュによりVPN情報が設定されたサービスプロファイルに関連するプロトコル群を制御するMAプロトコル処理部と、

そのサービスプロファイルに従ってサービス品質を保証するQoS制御とセキュリティゲートウェイ間のセキュリティを保証するためのトンネルを設定するMAVPN制御部と、

を有する付記1記載の装置。

(付記7) MAプロトコル処理部は、さらに配下のモバイルIPをサポートしない通信ホストに代わってホームネットワーク装置からの通信ホストへの結合更新メッセージを代理受信し、結合更新で通知されたVPN情報が設定されたサービスプロファイルを基に通信ホスト代わって他のネットワーク装置へのIPSec

c トンネルによるVPNパスを設定するプロトコル処理を実行する、付記6記載のシステム。

(付記8) モバイルIPネットワークにおけるVPNの設定方法は、

ー ユーザのネットワーク装置からそのホームエージェントに向けて静的なIPSecトンネルによるVPNパスを設定すること、

ー ユーザの移動端末から外部エージェントに位置登録要求メッセージを送信すること、

ー 外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

ー ホーム認証サーバは、受信した認証要求メッセージより自身のデータベースを参照して通信先ホスト、ネットワーク装置種別、及びユーザ別のセキュリティ・サービス情報を抽出して外部-ホームエージェント間及びユーザのネットワーク装置-ホームエージェント間のVPN情報をキャッシュし、それらを含む位置登録要求メッセージをホームエージェントに送信すること、

ー ホームエージェントは、受信した位置登録要求メッセージをキャッシュし、指定されたセキュリティ・サービスを設定し、ホームエージェントから通信先ホストであるユーザのネットワーク装置及び外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、位置登録処理の終了後に位置登録応答メッセージをホーム認証サーバに送信すること、

ー ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部-ホームエージェント間のVPN情報を付加した認証応答メッセージを外部エージェントのローカル認証サーバに送信すること、

ー ローカル認証サーバは、受信した認証応答メッセージをそのホーム-外部エージェント間のVPN情報をキャッシュしてから外部エージェントへ送信すること、

ー 外部エージェントは、受信した認証応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、外部エージェントからホームエージェントに向けたIPSecトンネルによるVPNパスを設定

した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、
から成ることを特徴とするVPNの設定方法。

(付記9) さらに、

ー ユーザの移動端末が同一ネットワーク内の新たな外部エージェントのエリアに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

ー 新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、ローカル認証サーバへ送信すること、

ー ローカル認証サーバは、キャッシュしてある外部-ホームエージェント間のVPN情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む認証応答メッセージを新外部エージェントに送信すること、

ー 新外部エージェントは、受信した位置登録要求メッセージをホームエージェントへ回送すること、

ー ホームエージェントは、受信した位置登録要求情報よりキャッシュしてある外部-ホームエージェント間のVPN情報の外部エージェント情報を新外部エージェントの情報に書き換え、ホームエージェントから旧外部エージェントに向けたVPNパスを削除し、指定されたセキュリティ・サービスを設定したホームエージェントから新外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、位置登録処理の終了後に位置登録応答メッセージを新外部エージェントに送信すること、

ー 新外部エージェントは、受信した位置登録応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、新外部エージェントからホームエージェントに向けたIPSecトンネルによるVPNパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、
を含む付記8記載の方法。

(付記10) さらに、

ー ユーザの移動端末が別のネットワーク内の新たな外部エージェントのエリアに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

－ 新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

－ ホーム認証サーバは、受信した認証要求メッセージよりキャッシュしてある外部－ホームエージェント間のVPN情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む位置登録要求メッセージをホームエージェントに送信すること、

－ ホームエージェントは、受信した位置登録要求情報によりキャッシュしてあるVPN情報を更新し、ホームエージェントから旧外部エージェントに向けたVPNパスを削除し、指定されたセキュリティ・サービスを設定したホームエージェントから新外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、位置登録処理の終了後に位置登録応答メッセージをホーム認証サーバに送信すること、

－ ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部－ホームエージェント間のVPN情報を付加した認証応答メッセージを新外部エージェントのローカル認証サーバに送信すること、

－ ローカル認証サーバは、受信した認証応答メッセージをキャッシュしてあるVPN情報を更新してから新外部エージェントへ回送すること、

－ 新外部エージェントは、受信した認証応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、及び新外部エージェントからホームエージェントに向けたIPSecトンネルによるVPNパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、を含む付記8記載の方法。

(付記11) モバイルIPネットワークにおけるVPNの設定方法は、

－ ユーザの移動端末から外部エージェントに位置登録要求メッセージを送信すること、

－ 外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

ー ホーム認証サーバは、受信した認証要求メッセージより自身のデータベースを参照して通信先ホスト、ネットワーク装置種別、及びユーザ別のセキュリティ・サービス情報を抽出し、ネットワーク装置種別がVPN動的設定可である場合はVPNキャッシュに外部エージェントー通信先ネットワーク装置のVPNを設定して、それらの情報を含む位置登録要求メッセージをホームエージェントに送信すること、

ー ホームエージェントは、受信した位置登録要求メッセージをキャッシュし、位置登録処理の終了後にネットワーク装置種別がVPN動的設定可である場合は通信先ホスト宛にこのVPN情報を付加した結合更新メッセージを送出すること、

ー ネットワーク装置は結合更新メッセージを代理受信し、それに付加されたVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、ネットワーク装置から外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、その後に結合承認メッセージをホームエージェントに送信すること、

ー ホームエージェントは、結合承認メッセージを受信すると、位置登録応答メッセージをホーム認証サーバへ送信すること、

ー ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部エージェントーネットワーク装置間のVPN情報を付加した認証応答メッセージを外部エージェントのローカル認証サーバに送信すること、

ー ローカル認証サーバは、受信した認証応答メッセージをその付加されたVPN情報をキャッシュしてから外部エージェントへ送信すること、

ー 外部エージェントは、受信した認証応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、外部エージェントからネットワーク装置に向けたIPSecトンネルによるVPNパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、

から成ることを特徴とするVPNの設定方法。

(付記12) さらに、

ー ユーザの移動端末が同一ネットワーク内の新たな外部エージェントのエリ

アに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

- － 新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、ローカル認証サーバへ送信すること、

- － ローカル認証サーバは、キャッシュしてある外部エージェントーネットワーク装置間のVPN情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む認証応答メッセージを新外部エージェントに送信すること、

- － 新外部エージェントは、受信した位置登録要求メッセージをホームエージェントへ回送すること、

- － ホームエージェントは、受信した位置登録要求情報よりキャッシュしてある外部エージェントーネットワーク装置間のVPN情報の外部エージェント情報を新外部エージェントの情報に書き換え、ネットワーク装置種別がVPN動的設定可である場合は通信先ホスト宛にこのVPN情報を付加した結合更新メッセージを送出すること、

- － ネットワーク装置は受信した結合更新メッセージよりキャッシュしてあるVPN情報を更新し、ネットワーク装置から旧外部エージェントに向けたVPNパスを削除し、指定されたセキュリティ・サービスを設定したネットワーク装置から新外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、その後に結合承認メッセージをホームエージェントに送信すること、

- － ホームエージェントは、結合承認メッセージを受信すると、位置登録応答メッセージを新外部エージェントへ送信すること、

- － 新外部エージェントは、受信した位置登録応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、新外部エージェントからネットワーク装置に向けたIPSecトンネルによるVPNパスを設定した後、ユーザの移動端末へ位置登録応答メッセージを返送すること、

を含む付記11記載の方法。

（付記13）さらに、

- － ユーザの移動端末が別のネットワーク内の新たな外部エージェントのエリ

アに移動し、そこから旧外部エージェントの位置情報を含む位置登録要求メッセージを送信すること、

ー 新外部エージェントは受信した位置登録要求情報を含む認証要求メッセージを、自身のローカル認証サーバを介してユーザのホーム認証サーバへ送信すること、

ー ホーム認証サーバは、受信した認証要求メッセージよりキャッシュしてある外部エージェントーネットワーク装置間のVPN情報の外部エージェント情報を新外部エージェントの情報に書き換え、その情報を含む位置登録要求メッセージをホームエージェントに送信すること、

ー ホームエージェントは、受信した位置登録要求情報によりキャッシュしてあるVPN情報を更新し、ネットワーク装置種別がVPN動的設定可である場合は通信先ホスト宛にこのVPN情報を付加した結合更新メッセージを送出すること、

ー ネットワーク装置は受信した結合更新メッセージよりキャッシュしてあるVPN情報を更新し、ネットワーク装置から旧外部エージェントに向けたVPNパスを削除し、指定されたセキュリティ・サービスを設定したネットワーク装置から新外部エージェントに向けたIPSecトンネルによるVPNパスを設定し、その後に結合承認メッセージをホームエージェントに送信すること、

ー ホームエージェントは、結合承認メッセージを受信すると、位置登録応答メッセージをホーム認証サーバへ送信すること、

ー ホーム認証サーバは、位置登録応答メッセージの受信により、キャッシュしてある外部エージェントーネットワーク装置間のVPN情報を付加した認証応答メッセージを新外部エージェントのローカル認証サーバに送信すること、

ー ローカル認証サーバは、受信した認証応答メッセージをその付加されたVPN情報をキャッシュしてから新外部エージェントへ回送すること、

ー 新外部エージェントは、受信した認証応答メッセージに含まれるVPN情報をキャッシュし、指定されたセキュリティ・サービスを設定し、新外部エージェントからネットワーク装置に向けたIPSecトンネルによるVPNパスを設定した後、ユーザの移動端末へ登録応答メッセージを返送すること、

を含む付記 1 1 記載の方法。

(付記 1 4) さらに、

- － 新外部エージェントは、キャッシュしてある VPN 情報を複写して、送信元を旧外部エージェント及び送信先を新外部エージェントに書き換えた VPN 情報を付加した結合更新メッセージを旧外部エージェントへ送信すること、

- － 旧外部エージェントは、受信した結合更新メッセージの VPN 情報をキャッシュし、旧外部エージェントからホームエージェントに向けた VPN パスを削除し、指定されたセキュリティ・サービスを設定した旧外部エージェントから新外部エージェントに向けた IPsec トンネルによる VPN パスを設定した後、新外部エージェントへ結合承認メッセージを送信すること、

を含む付記 9 又は 1 2 記載の方法。

(付記 1 5) さらに、

- － 新外部エージェントは、認証応答メッセージに旧外部エージェントの情報が含まれている時は、キャッシュしてある VPN 情報を複写して、送信元を旧外部エージェント及び送信先を新外部エージェントに書き換えた VPN 情報を付加した結合更新メッセージを旧外部エージェントへ送信すること、

- － 旧外部エージェントは、受信した結合更新メッセージの VPN 情報をキャッシュし、旧外部エージェントからホームエージェントに向けた VPN パスを削除し、指定されたセキュリティ・サービスを設定した旧外部エージェントから新外部エージェントに向けた IPsec トンネルによる VPN パスを設定した後、新外部エージェントへ結合確認メッセージを送信すること、

を含む付記 1 0 又は 1 3 記載の方法。

(付記 1 6) さらに、

- － ユーザが所定の通信手段によりそのホーム認証サーバのデータベースへアクセスしてユーザの VPN 情報をカスタマイズし、それによりネットワーク装置種別が VPN 動的設定可であるネットワーク装置に通信先を変更すること、

- － ユーザの移動端末から外部エージェントにサービス更新要求を付加した位置登録要求メッセージを送信すること、

を含む付記 1 1 記載の方法。

(付記 1 7) さらに、

ー ネットワーク装置は配下の通信ホストのライフタイムを計測し、残りのライフタイムが所定閾値以下になった時にそのVPN情報を通知してきたホームエージェントに結合要求メッセージを送信し、結合更新メッセージを受信しない場合には前記VPN情報を削除すること、

ー ホームエージェントは受信した結合要求メッセージに含まれるユーザの移動端末の情報からキャッシュしてあるVPN情報を検索し、前記ネットワーク装置の情報が存在する場合は結合更新メッセージを送信し、存在しない場合には放置すること、

を含む付記 1 6 記載の方法。

【0 0 9 8】

【発明の効果】

以上説明したように、本発明によれば以下に示す効果が奏される。

1) モバイルIPにおける位置登録手順に連携して、通信に参与する端末の公衆IPネットワークへのセキュリティゲートウェイに動的にIPSecを用いたVPNを設定する事で、MNやCNにVPN用の特殊な機能を持たせる事無しに、任意の端末間でのVPN設定サービスの提供を可能にする。

2) ユーザが自由に組み合わせて指定したサービス品質、セキュリティレベル、経路でのVPN設定を可能にする。

3) MNの移動に伴い、VPNの経路を自動更新することを可能にする。

【図面の簡単な説明】

【図 1】

既存提案によるモバイルIP+IPSecの適用例を示した図である。

【図 2】

本発明によるネットワーク構成の一例を示した図である。

【図 3】

本発明の機能ブロック構成例を示した図である。

【図 4】

本発明の第 1 の実施例を示した図である。

【図 5】

VPNデータベースの構成例を示した図である。

【図 6】

AAAの詳細機能ブロック構成例を示した図である。

【図 7】

VPN情報キャッシュの構成例を示した図である。

【図 8】

CN-GWアドレス対応表を示した図である。

【図 9】

AAAの全体処理フロー例を示した図である。

【図 1 0】

AAAプロトコル処理部の処理フロー例を示した図である。

【図 1 1】

図 1 0 でのメッセージ対応表を示した図である。

【図 1 2】

AAAVPN制御部の処理フロー例を示した図である。

【図 1 3】

VPN経路決定制御部の処理フロー例を示した図である。

【図 1 4】

MA (FA, HA, PCN) の詳細機能ブロック例を示した図である。

【図 1 5】

IPSec情報テーブルの構成例を示した図である。

【図 1 6】

ルートテーブルの構成例を示した図である。

【図 1 7】

MAの全体処理フロー例を示した図である。

【図 1 8】

MAプロトコル処理部の処理フロー例を示した図である。

【図 1 9】

AAAプロトコル処理部の処理フロー例を示した図である。

【図 2 0】

モバイルIPプロトコル処理部の処理フロー例を示した図である。

【図 2 1】

図 2 0 でのメッセージ対応表を示した図である。

【図 2 2】

MAVPN制御部の処理フロー例を示した図である。

【図 2 3】

QoS制御部の処理フロー例を示した図である。

【図 2 4】

トンネル制御部の処理フロー例を示した図である。

【図 2 5】

本発明の第 2 の実施例を示した図である。

【図 2 6】

本発明の第 3 の実施例を示した図である。

【図 2 7】

本発明の第 4 の実施例を示した図である。

【図 2 8】

本発明の第 5 の実施例を示した図である。

【図 2 9】

本発明の第 6 の実施例を示した図である。

【図 3 0】

本発明の第 7 の実施例を示した図である。

【符号の説明】

1 … モバイルノード

2 ～ 5 … ISP ネットワーク

2 1、3 1、4 1、5 1 … セキュリティゲートウェイ

2 3、3 3 … AAA 認証サーバ

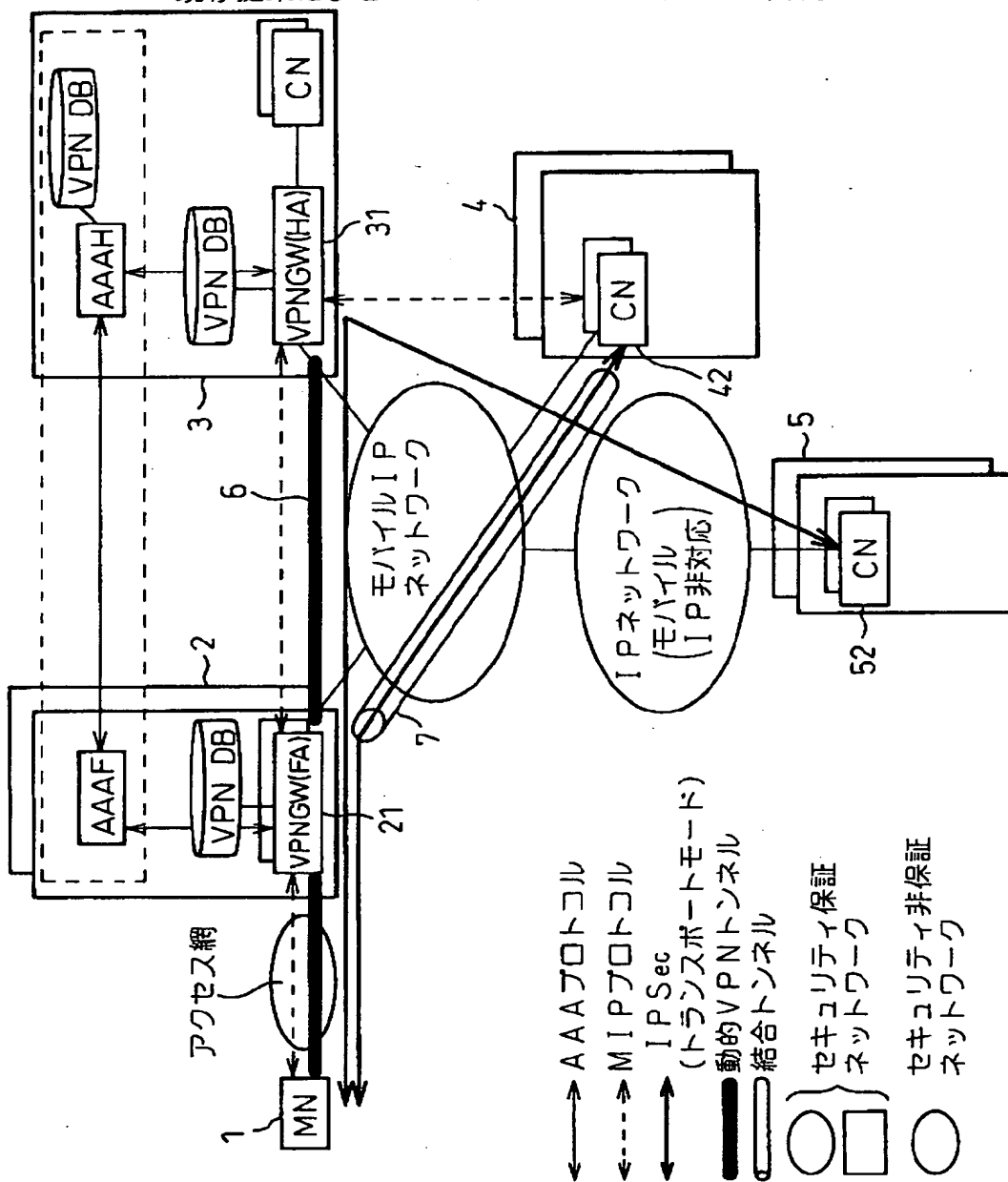
3 4 … VPN データベース

3 6 … ウェブアプリケーション

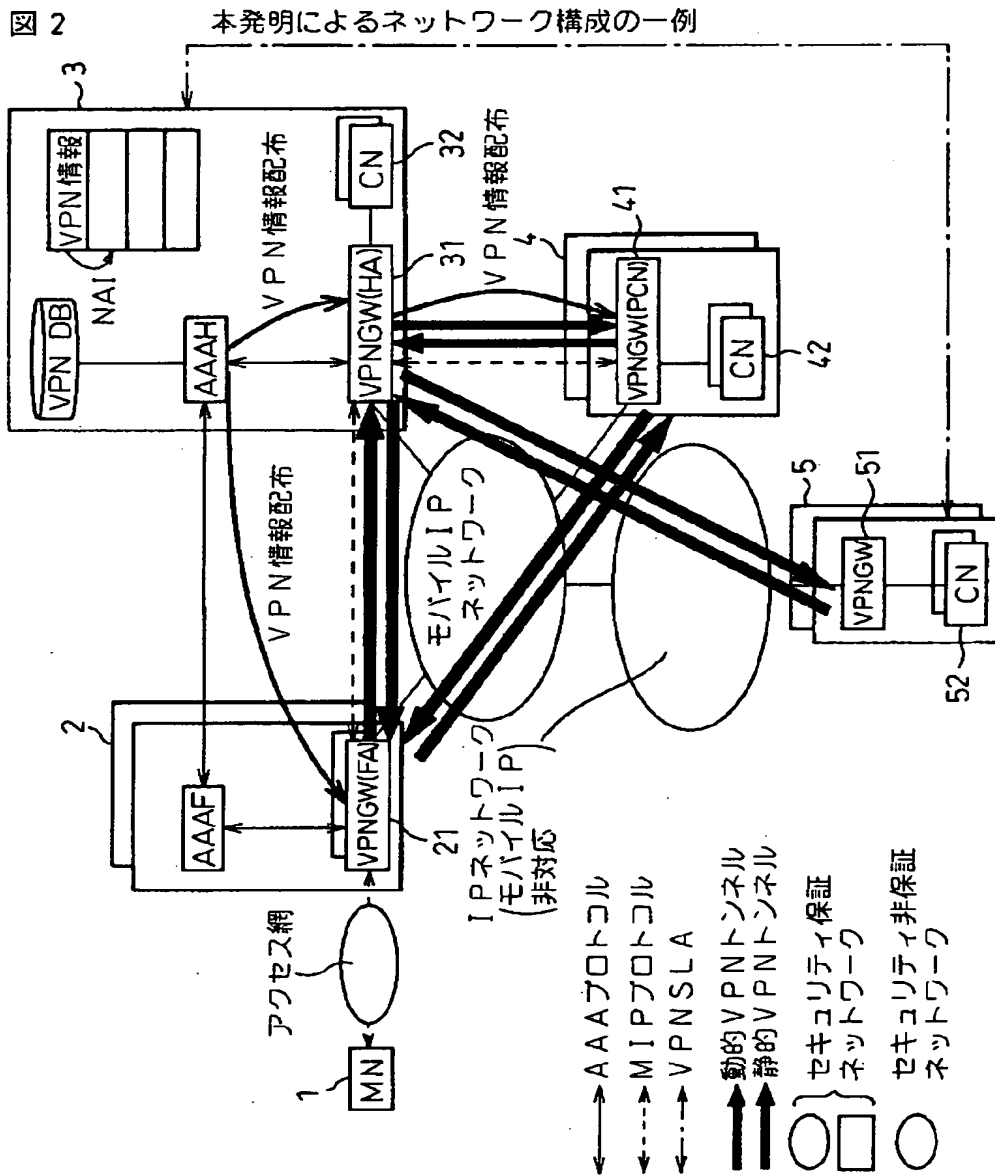
【書類名】 図面

【図 1】

図 1 既存提案によるモバイル IP + IP Sec の適用例

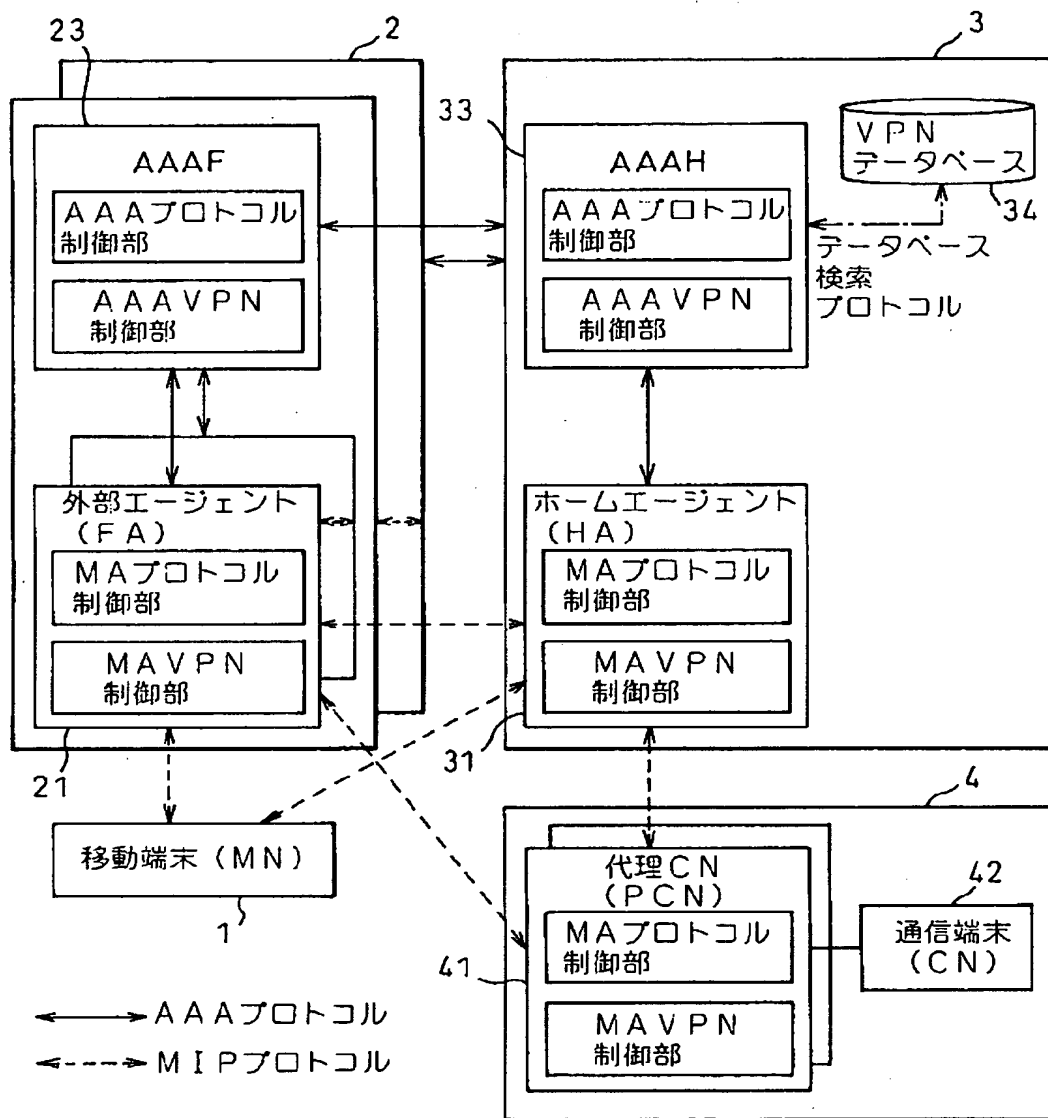


【図 2】

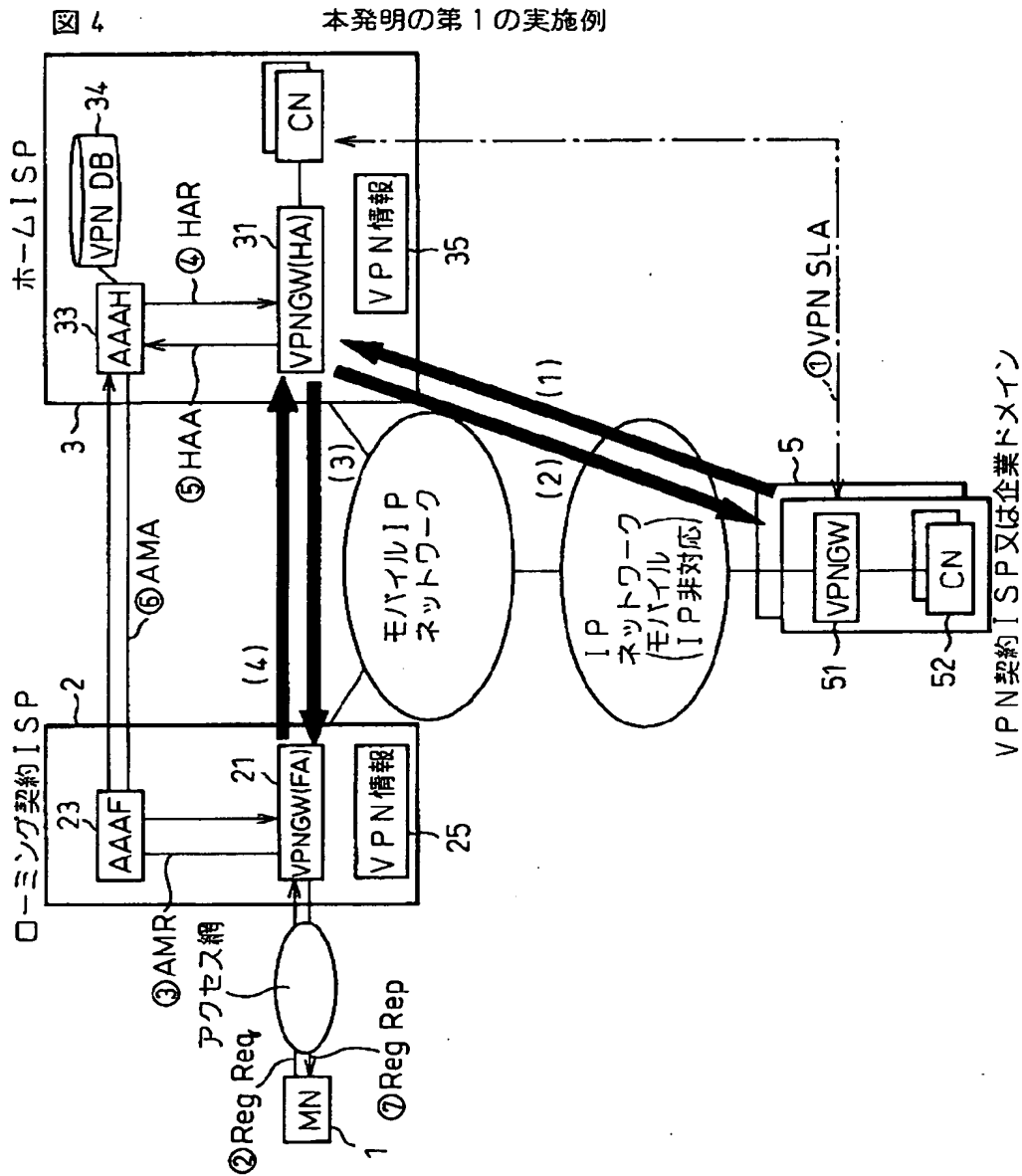


【図3】

図3 本発明の基本的な機能ブロック構成例



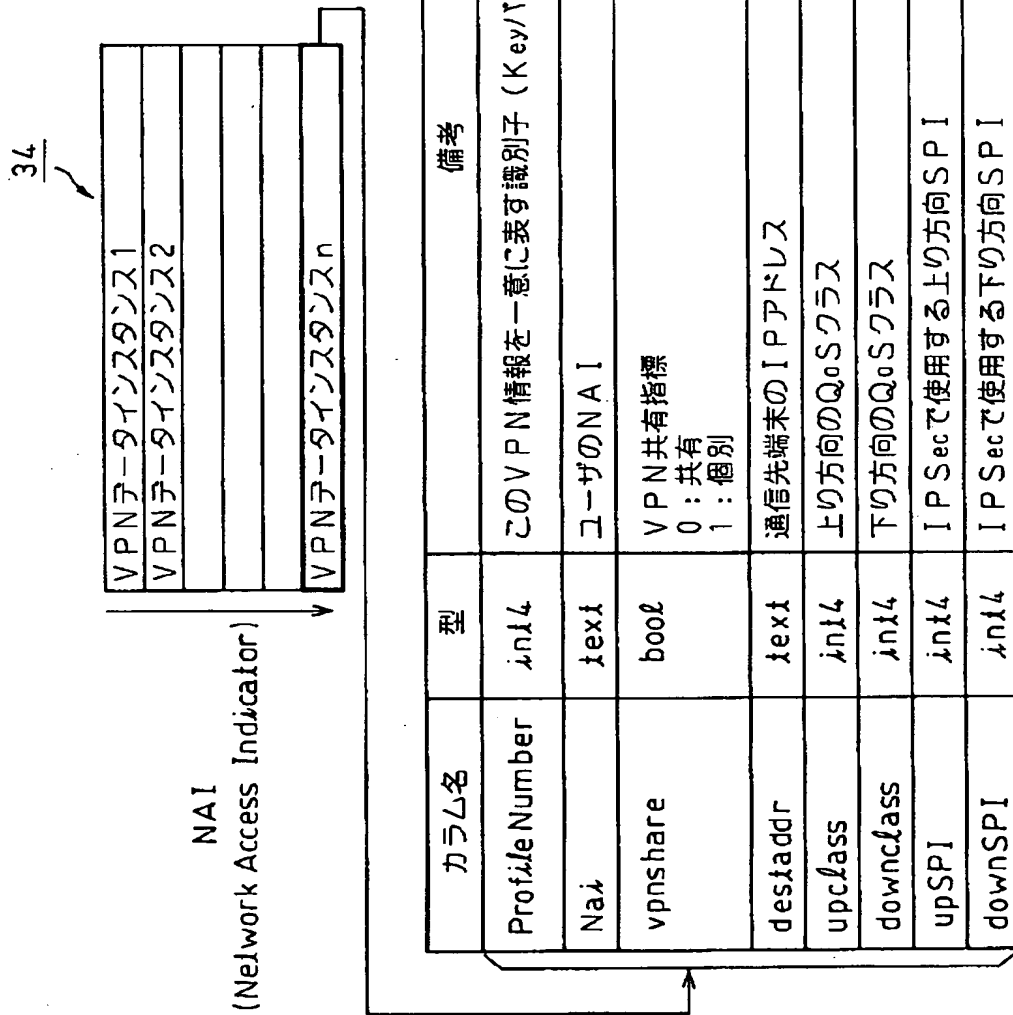
【図 4】



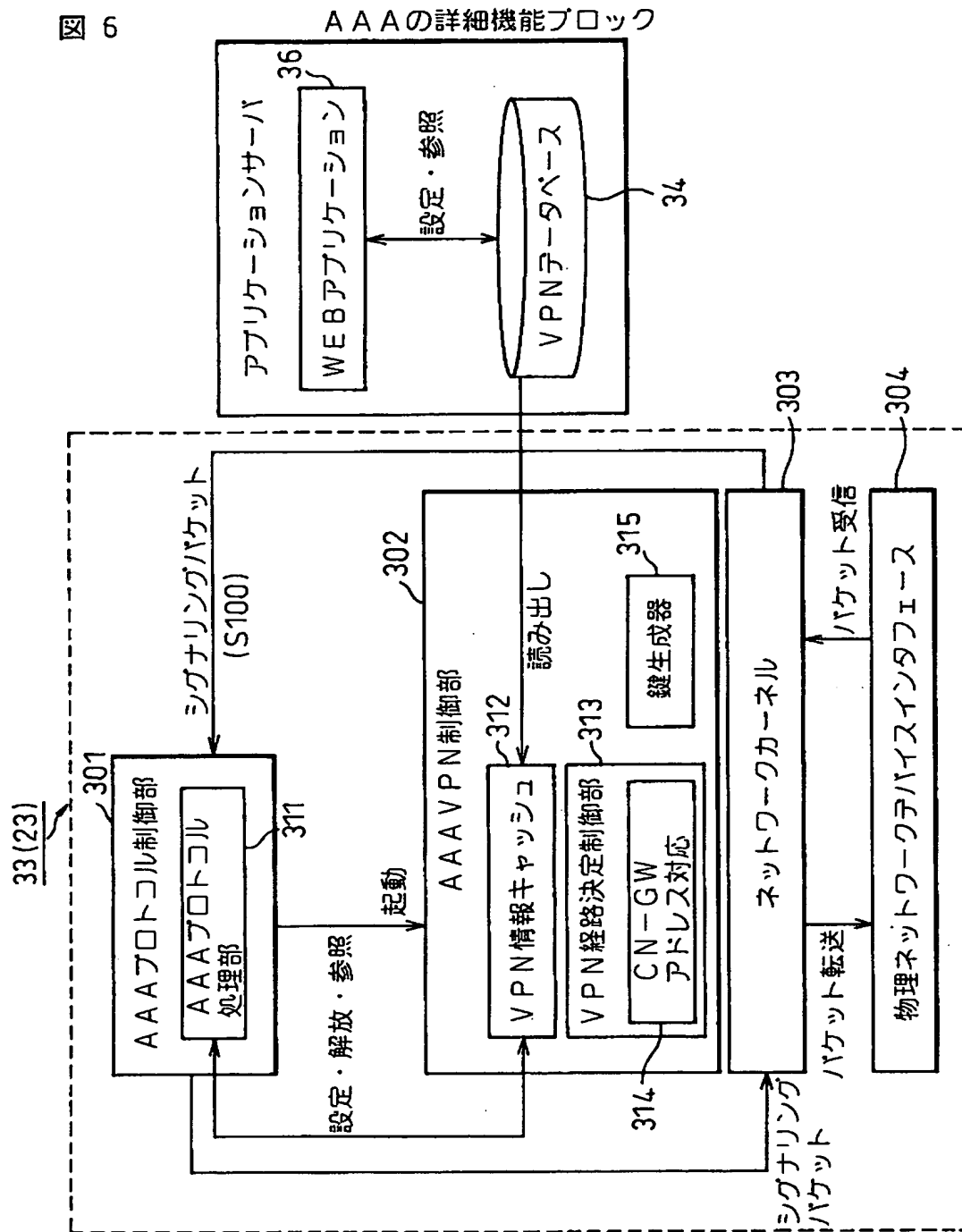
【図 5】

図 5

VPNデータベースの構成例



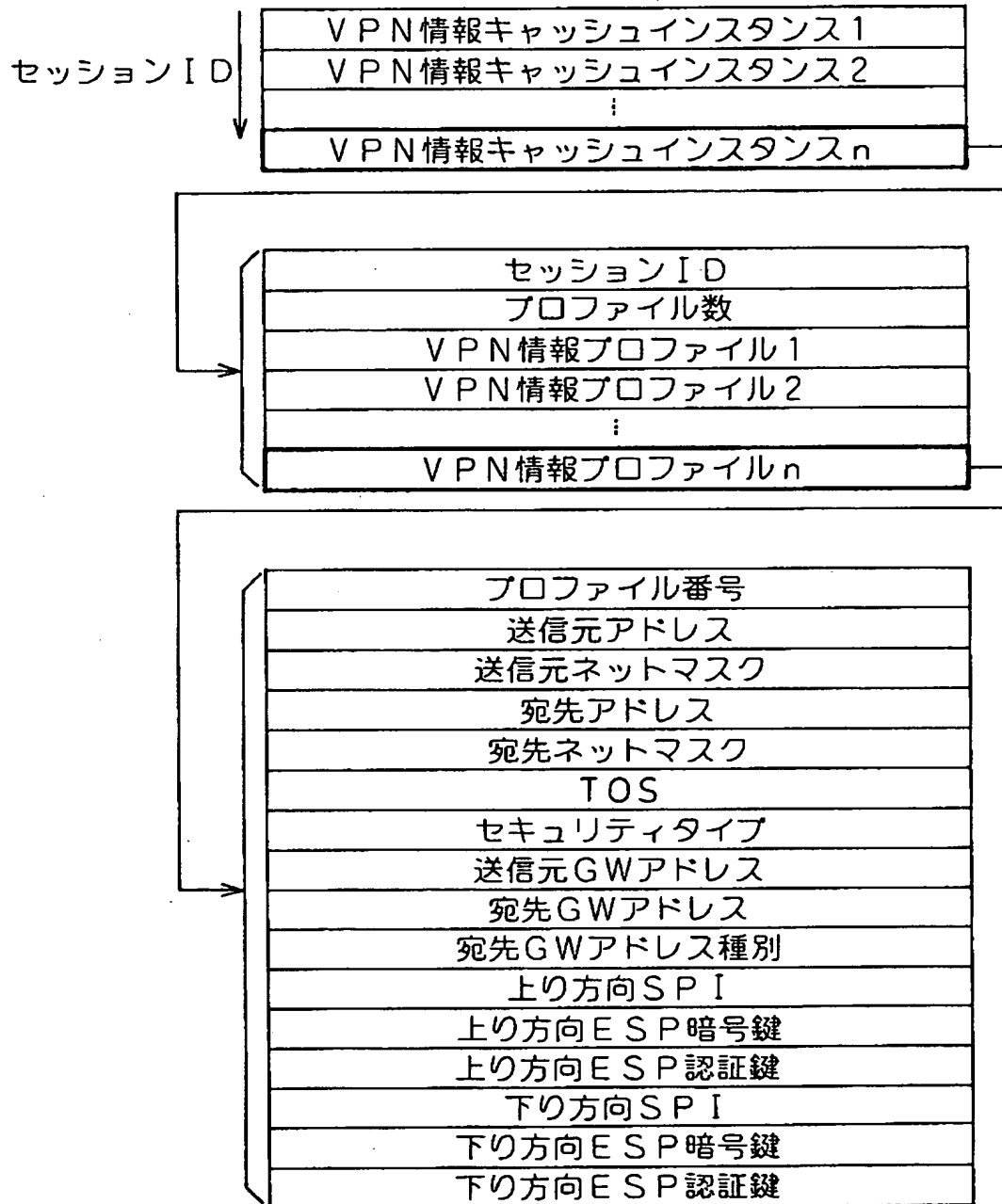
【図 6】



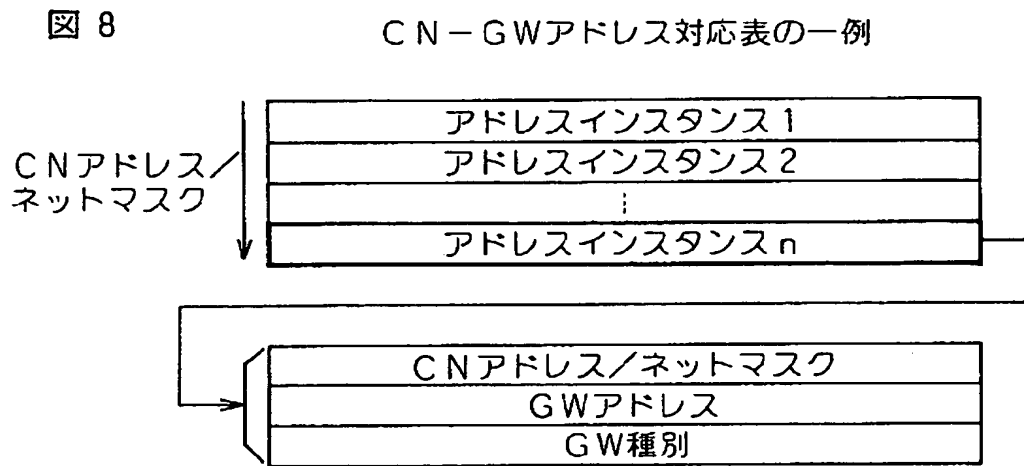
【図 7】

図 7

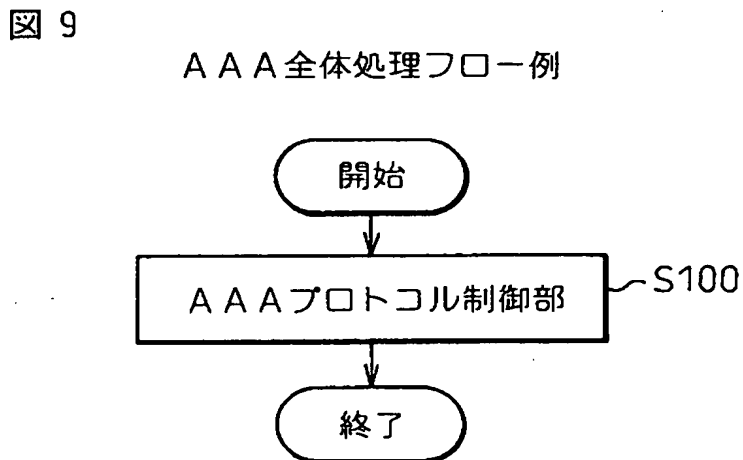
VPN情報キャッシュの一例



【図 8】

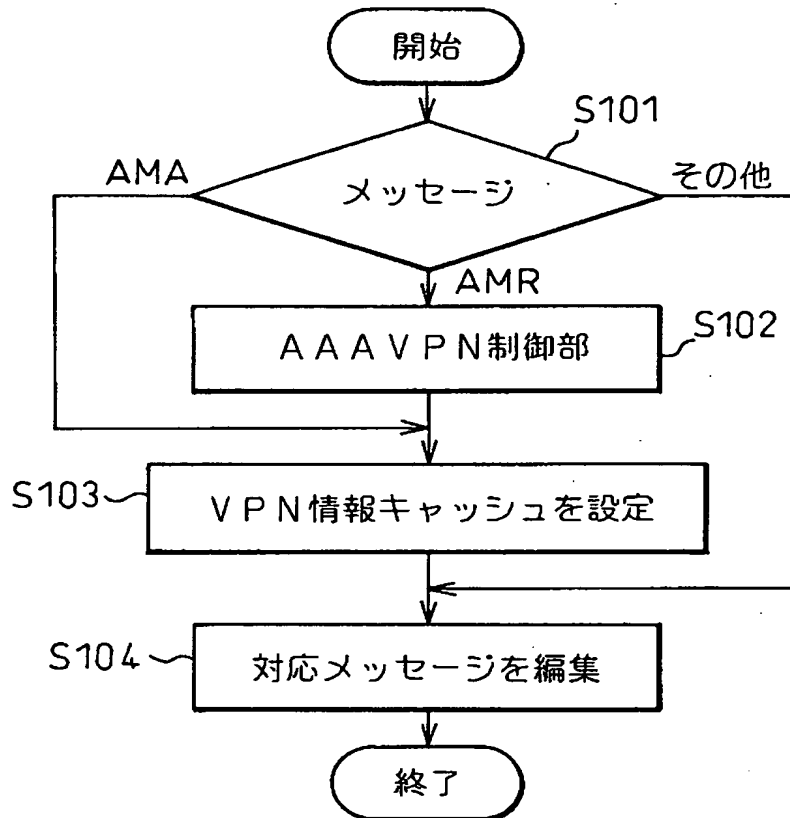


【図 9】



【図 1 0】

図 10 A A A プロトコル処理部の処理フロー例



【図 1 1】

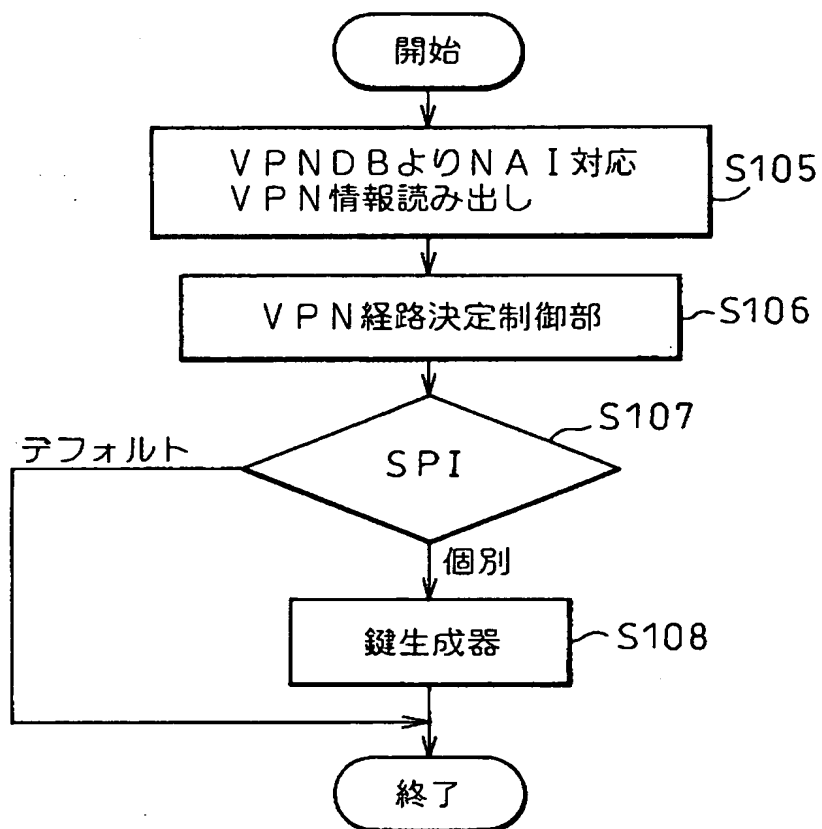
図 11 図10の S103でのメッセージ対応表

受信メッセージ	処理実行 A A A	送信メッセージ
AMR	AAAF	AMR
	AAAH	HAR
AMA	AAAF	AMA
HAA	AAAH	AMA

【図 1 2】

図 12

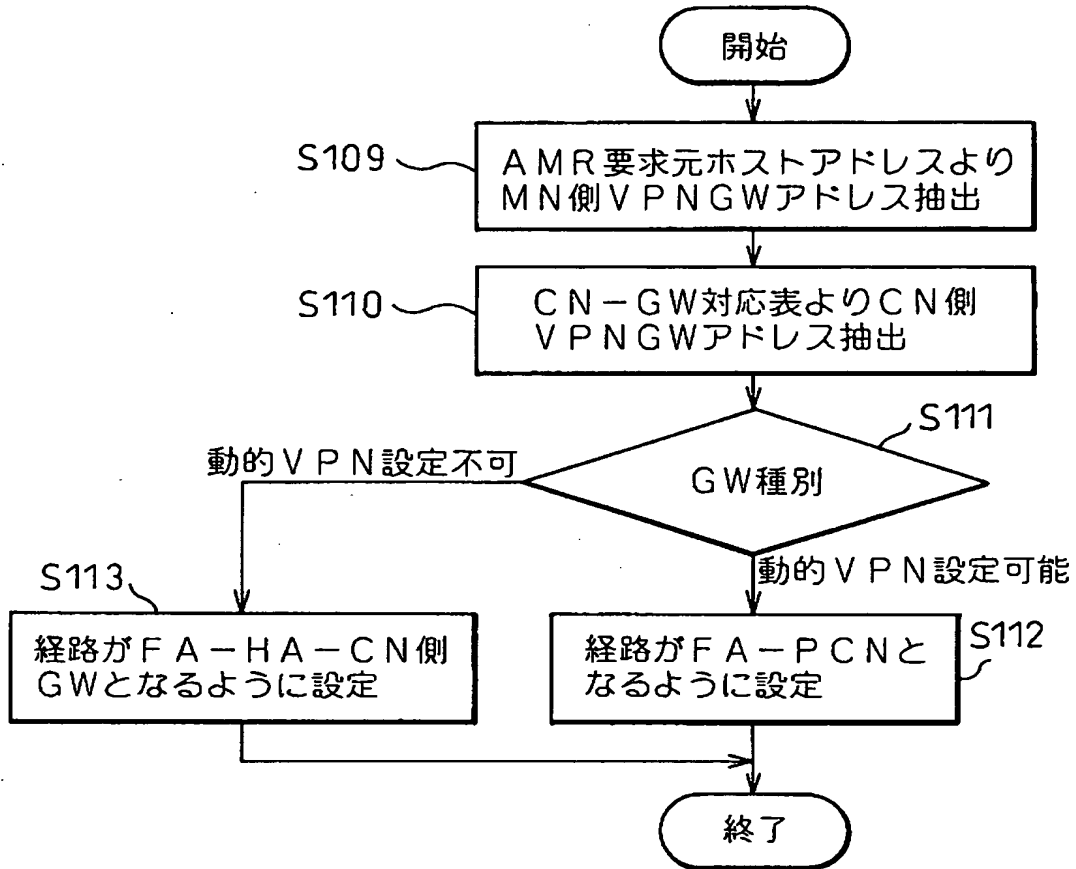
A A A V P N 制御部の処理フロー例



【図13】

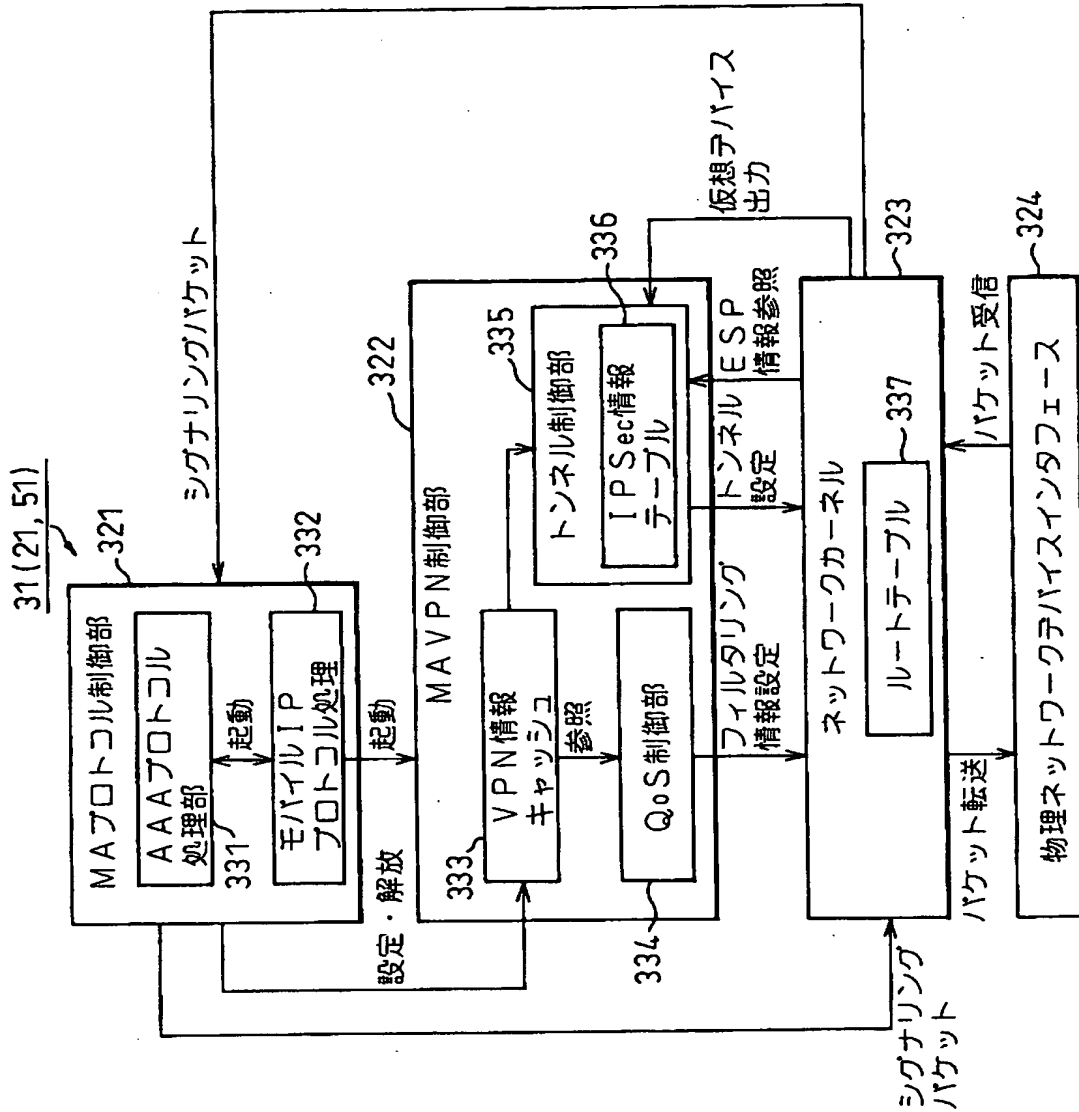
図13

VPN経路決定制御部の処理フロー例



【図14】

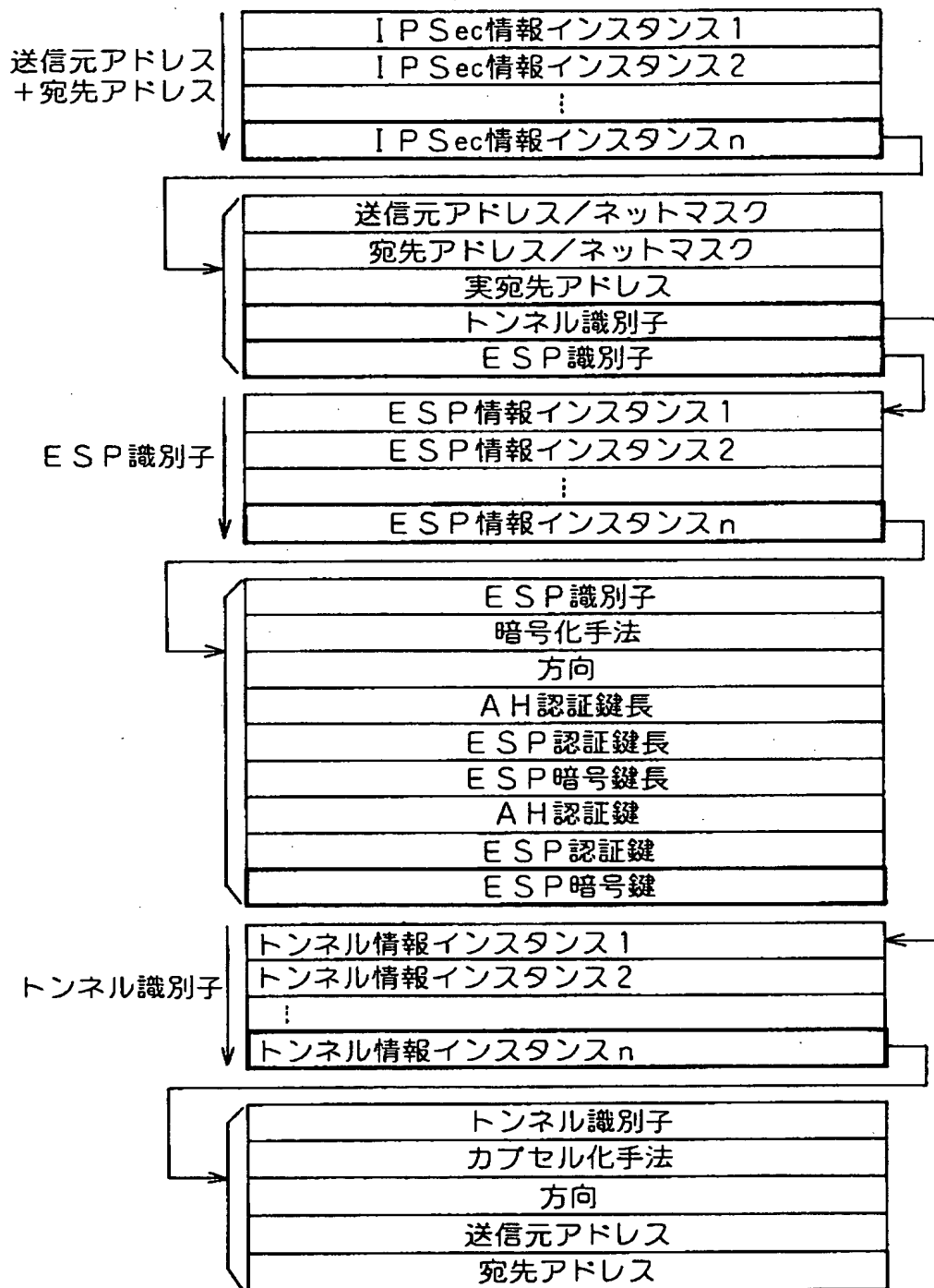
図14 MA (FA, HA, PCN) の詳細機能ブロック



【図 15】

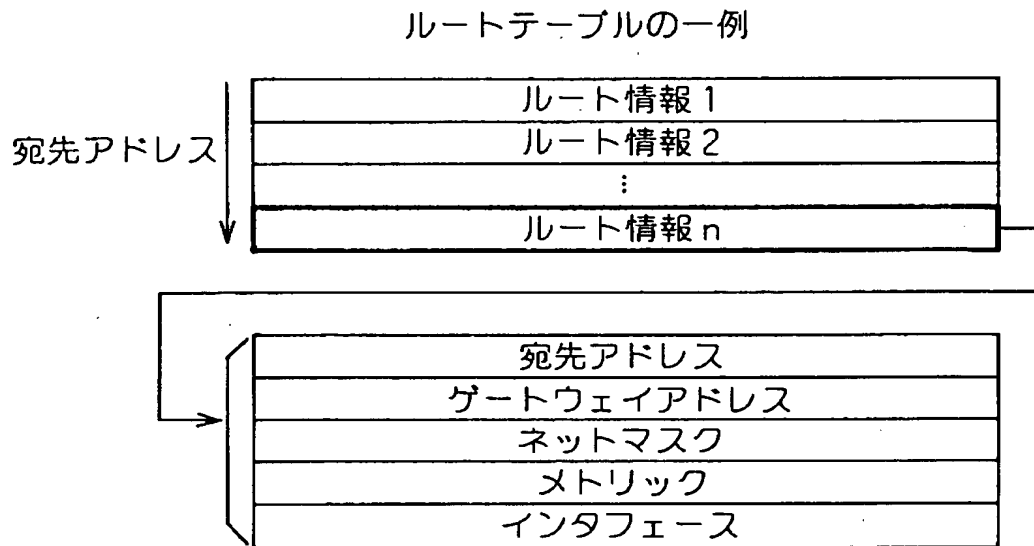
図 15

IPSec情報テーブルの一例



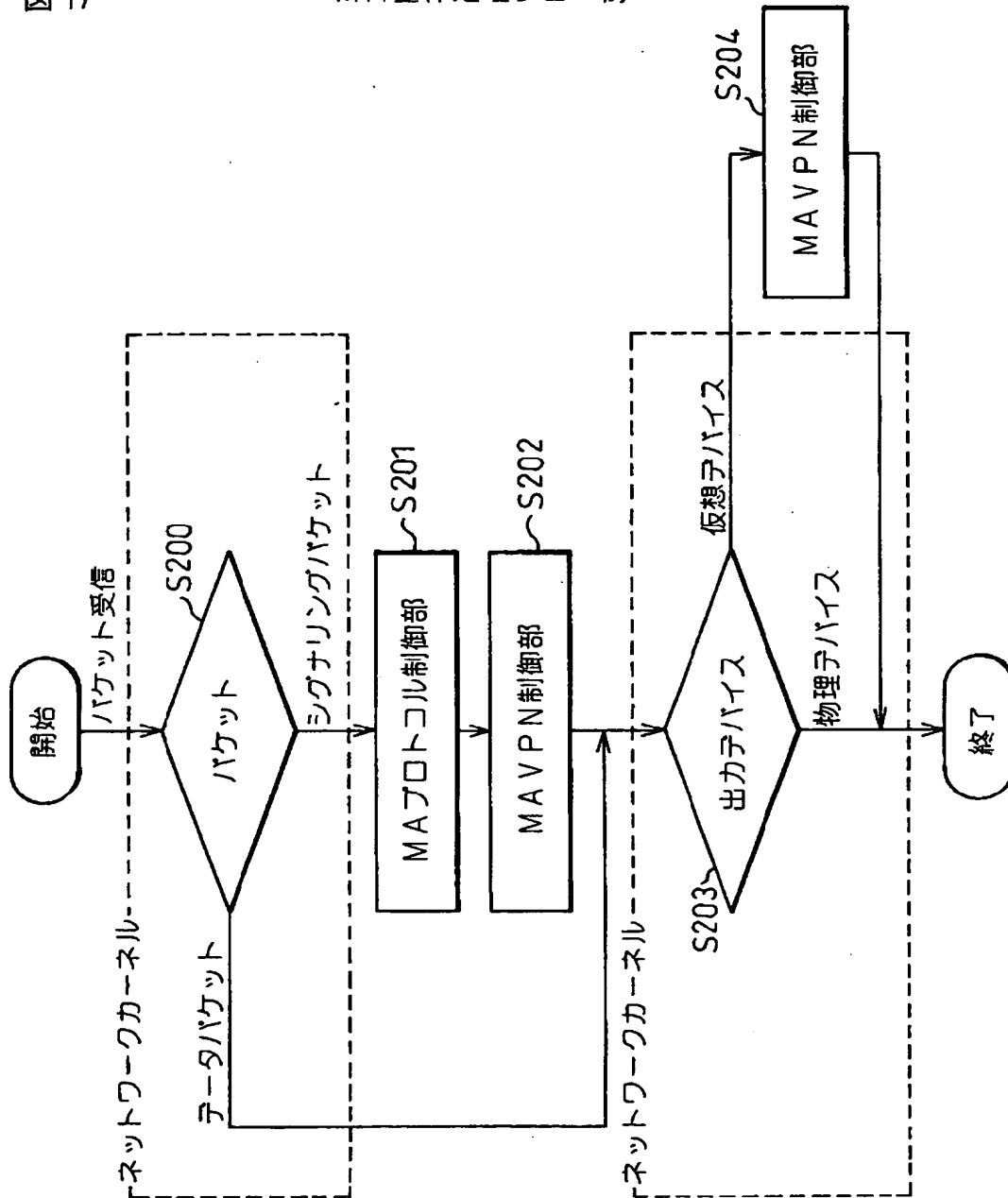
【図 16】

図 16



【図 17】

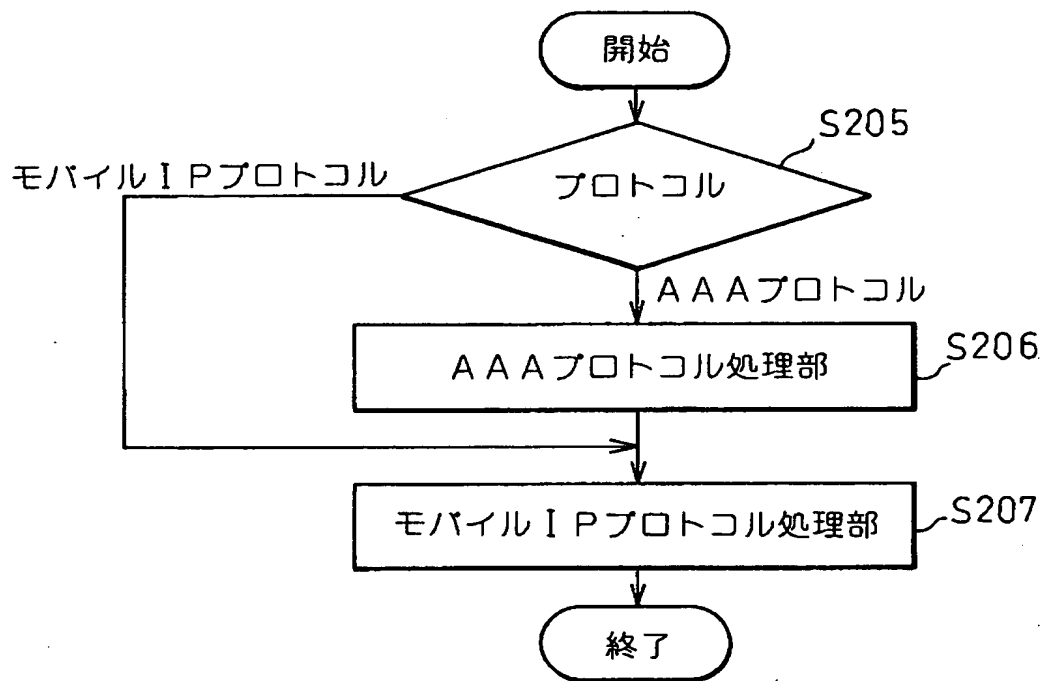
図 17 MA 全体処理フロー例



【図 1 8】

図 18

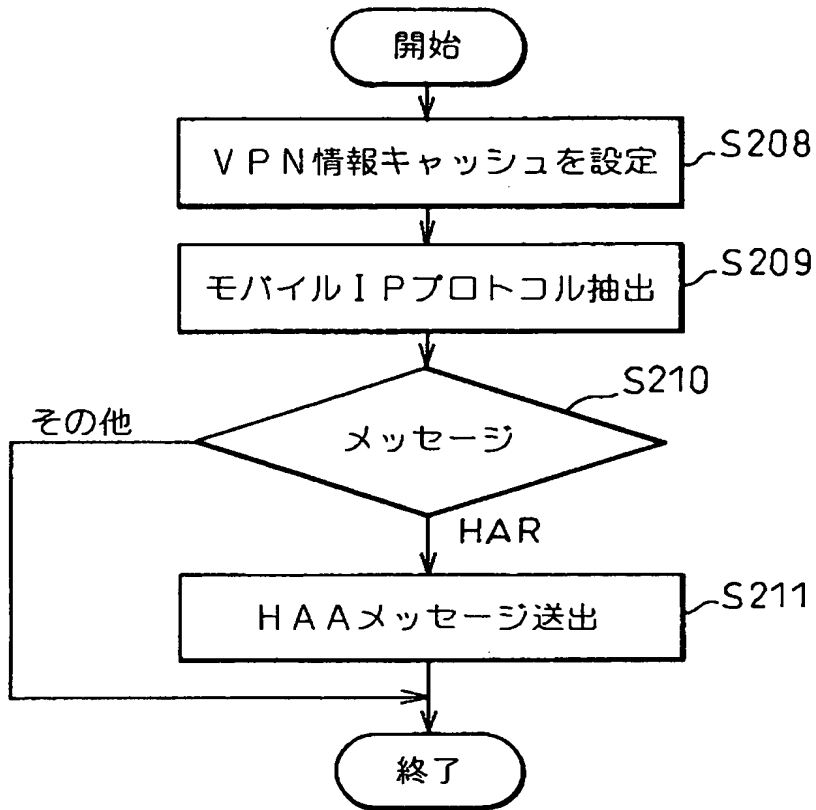
MA プロトコル制御の処理フロー例



【図 1 9】

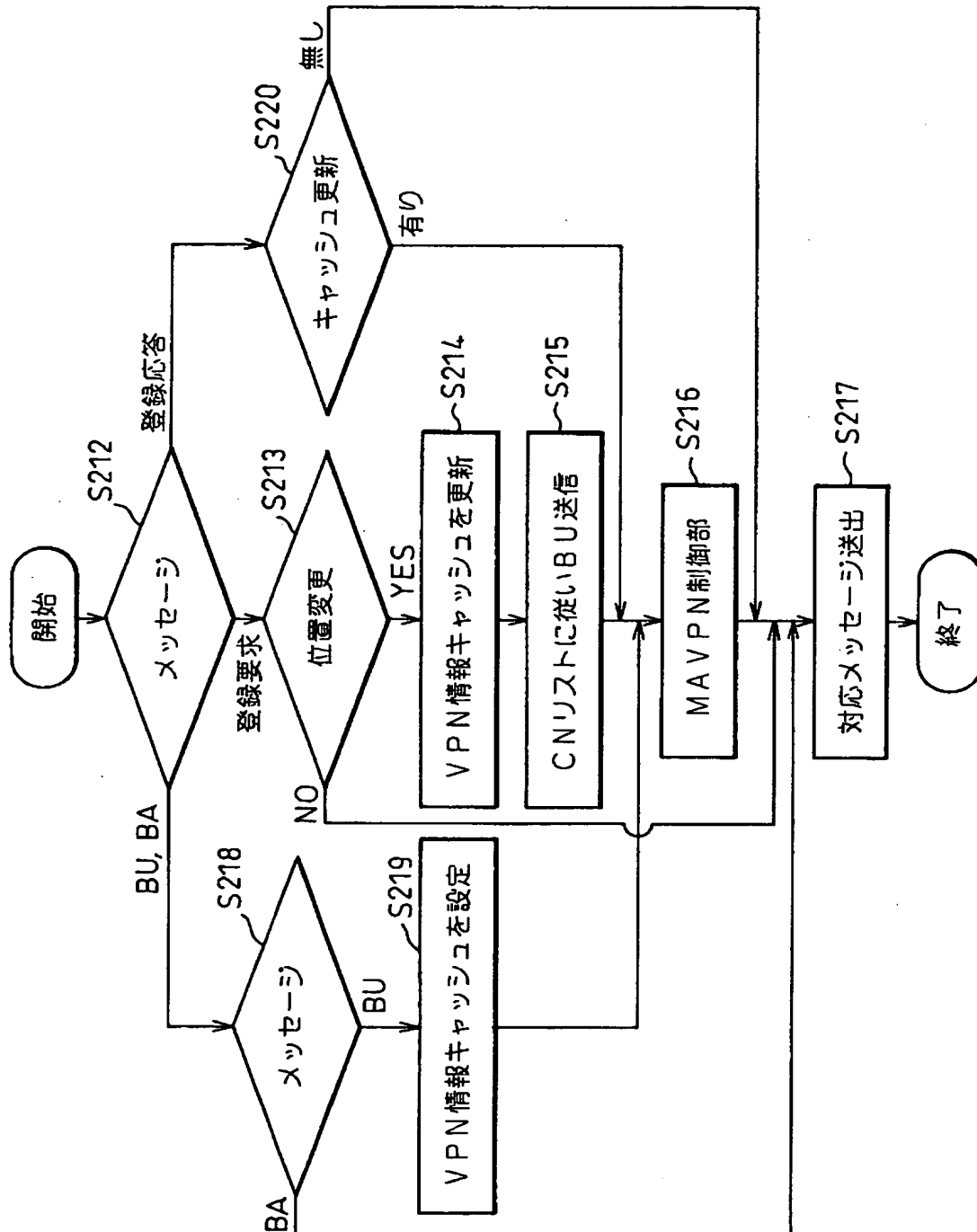
図 19

A A A プロトコル処理部の処理フロー例



【図 20】

図 20 モバイル IP プロトコル 処理部の処理フロー例



【図 2 1】

図 21

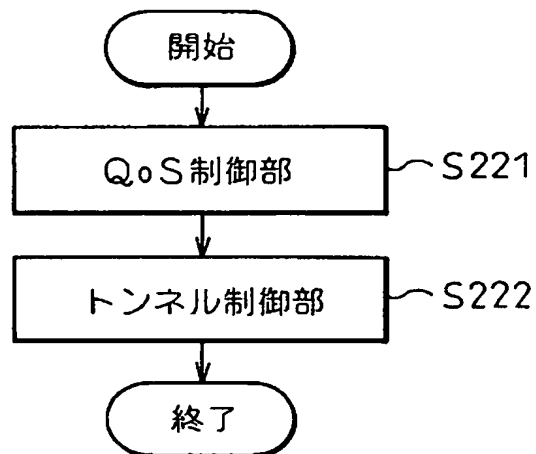
図20のS217でのメッセージ対応表

受信メッセージ	処理実行MA	送信メッセージ
登録要求	FA	登録応答
	HA	BU
登録応答	FA	登録応答
BU	FA, PCN	BA
BA	HA	登録応答

【図 2 2】

図 22

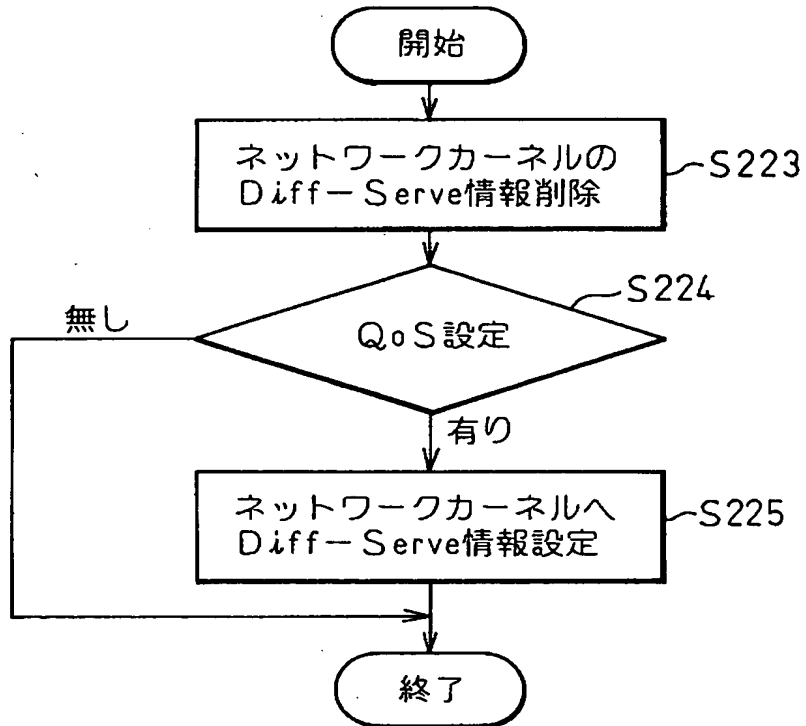
MAVPN制御部の処理フロー例



【図 2 3】

図 23

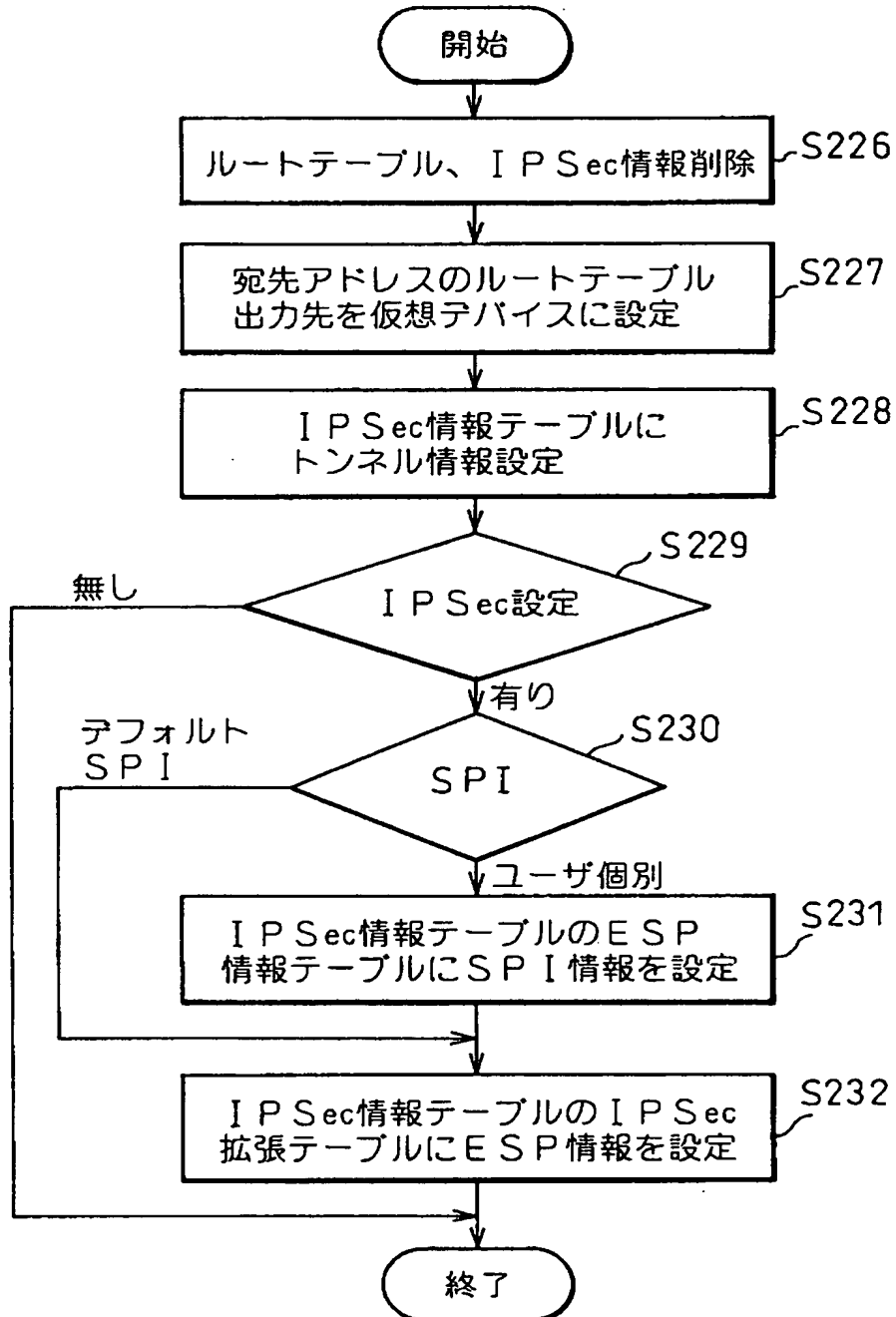
QoS制御部の処理フロー例



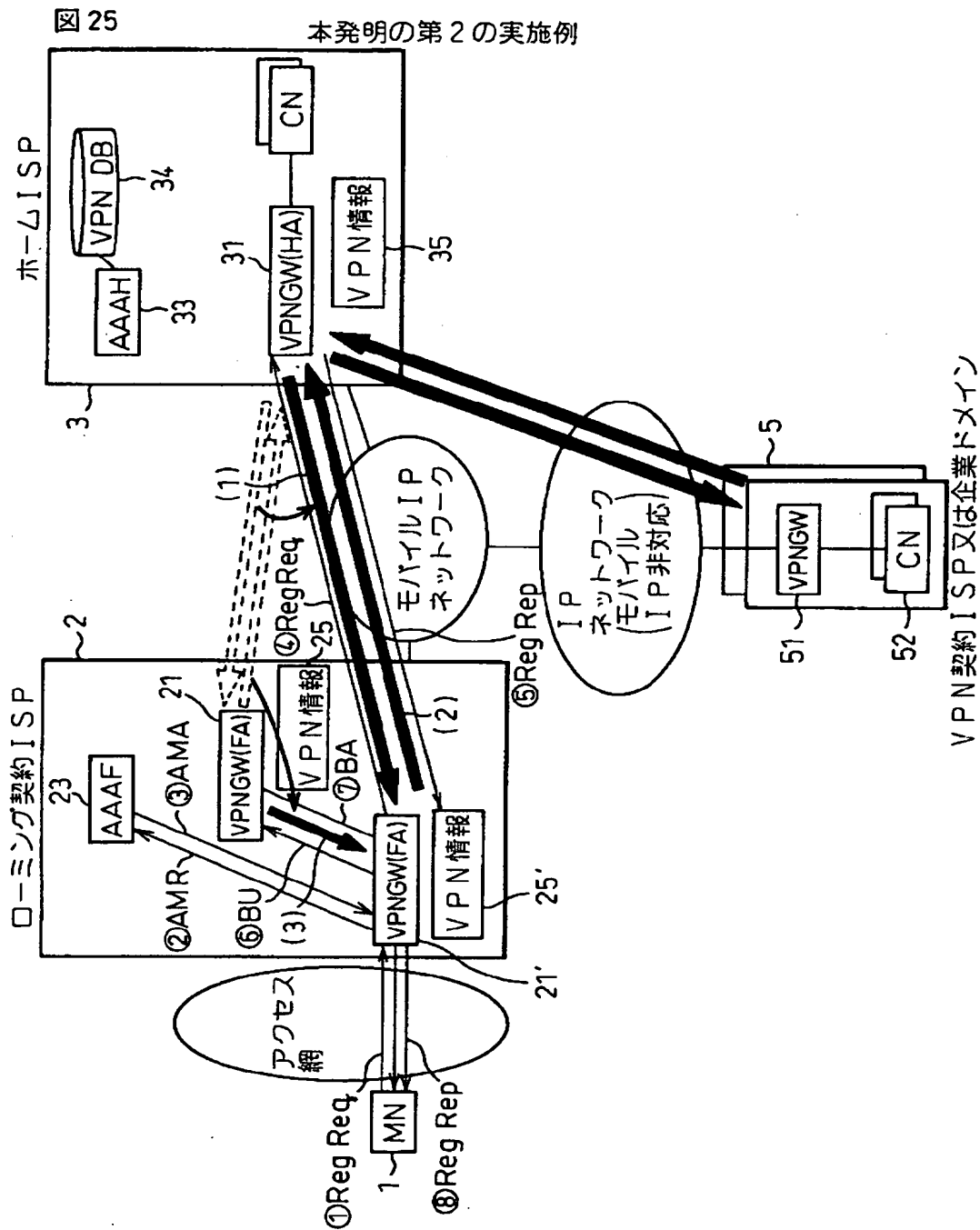
【図 24】

図 24

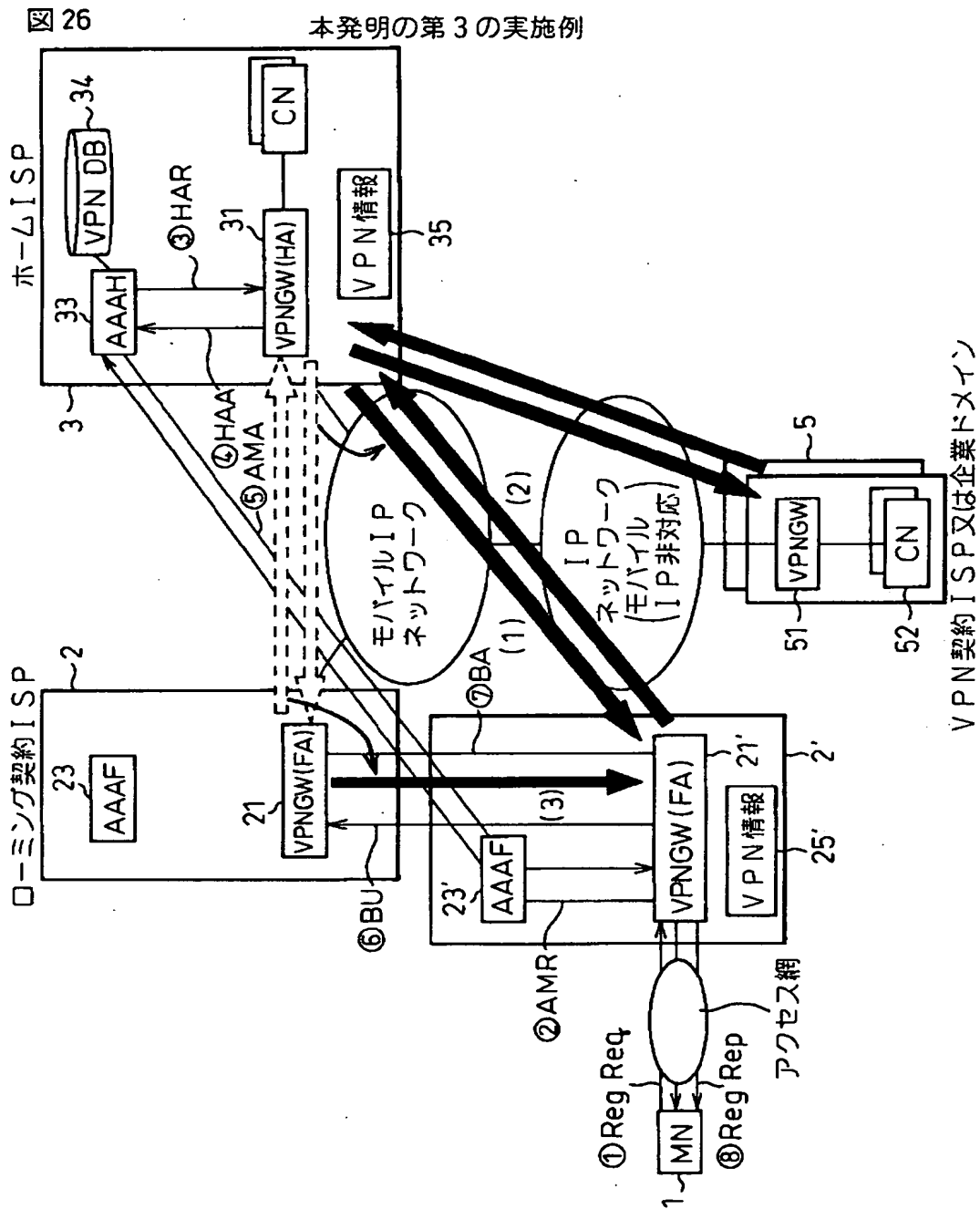
トンネル制御部の処理フロー例



【図 25】



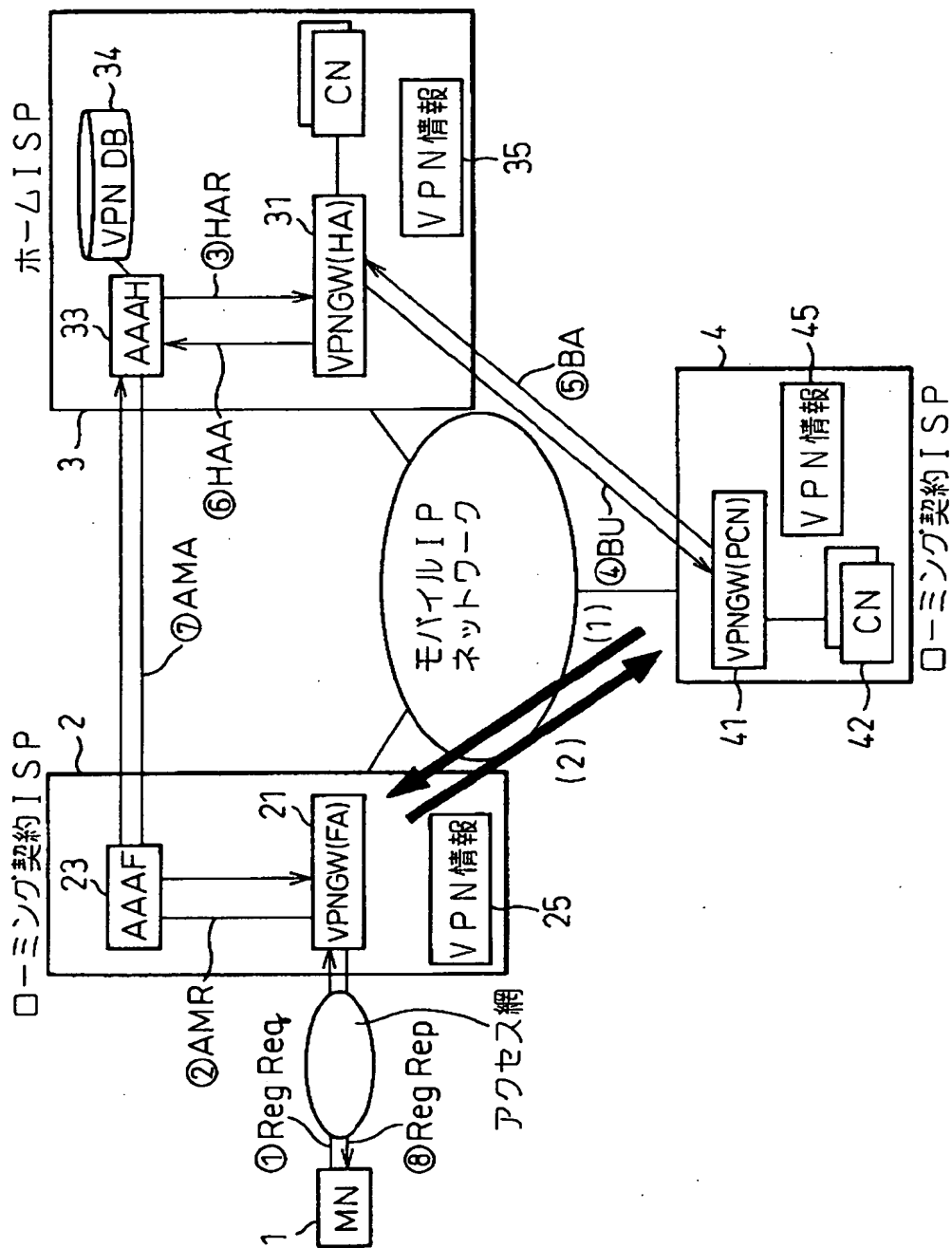
【図 26】



【図 27】

図 27

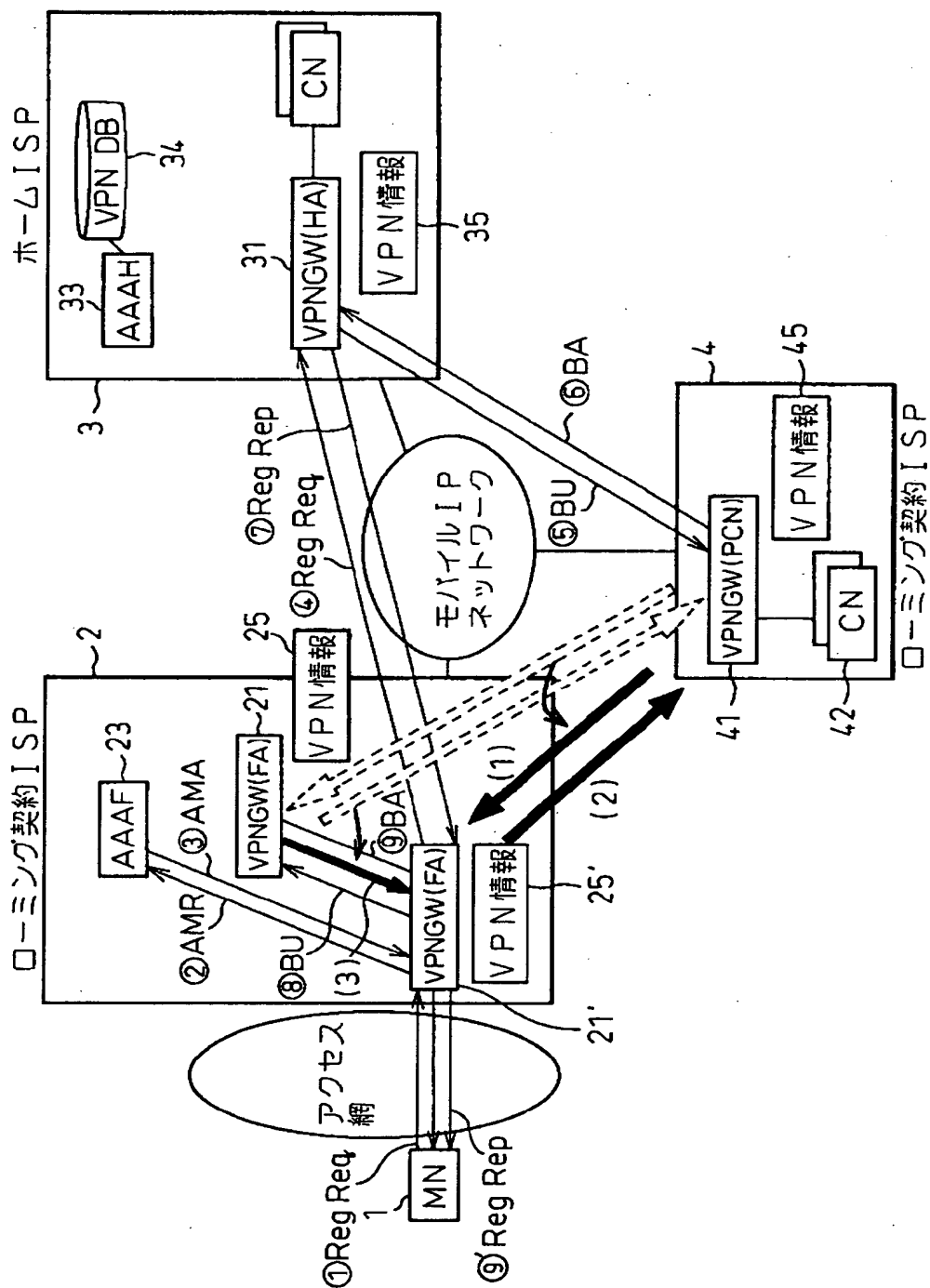
本発明の第 4 の実施例



【図 28】

図 28

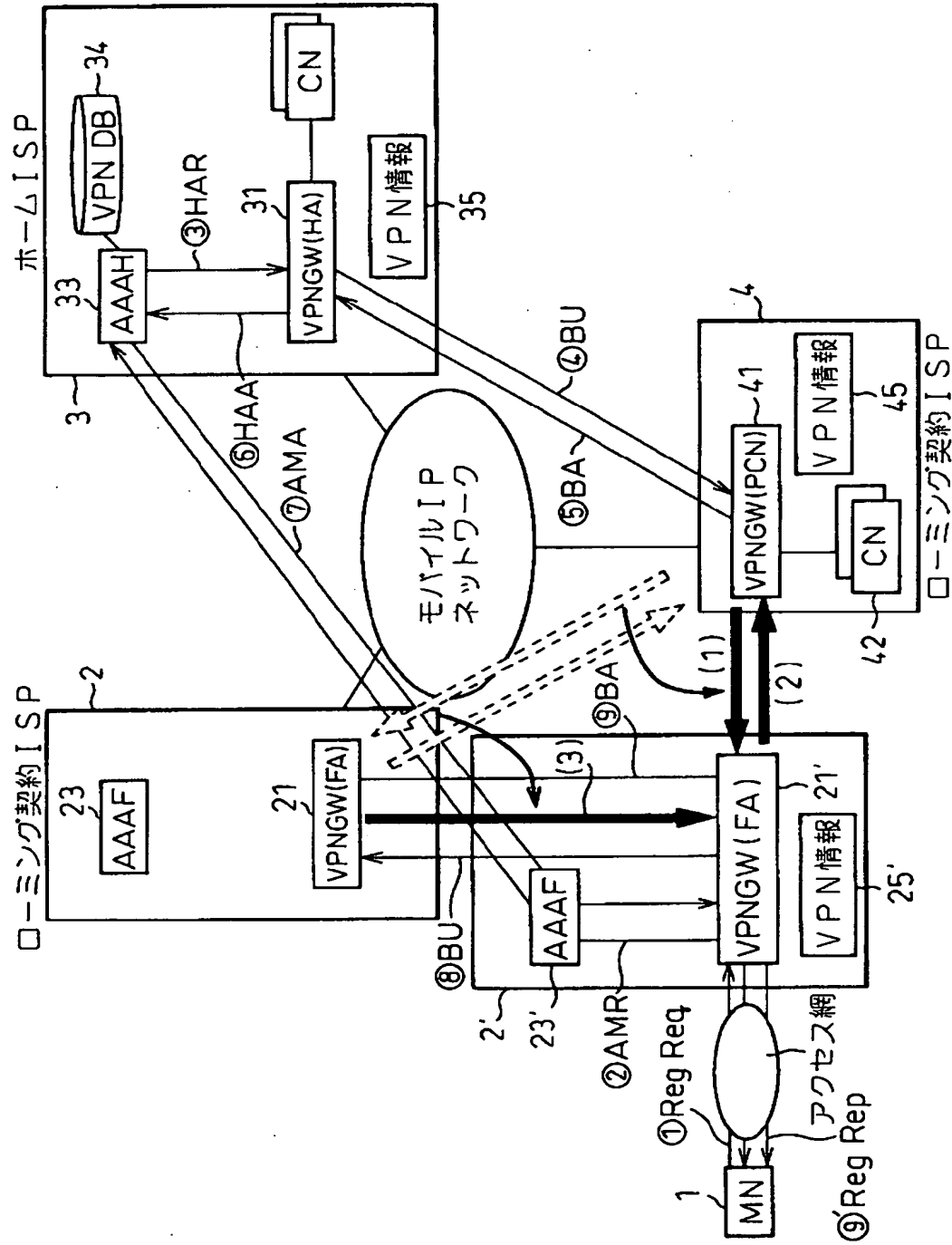
本発明の第 5 の実施例



【図 29】

図 29

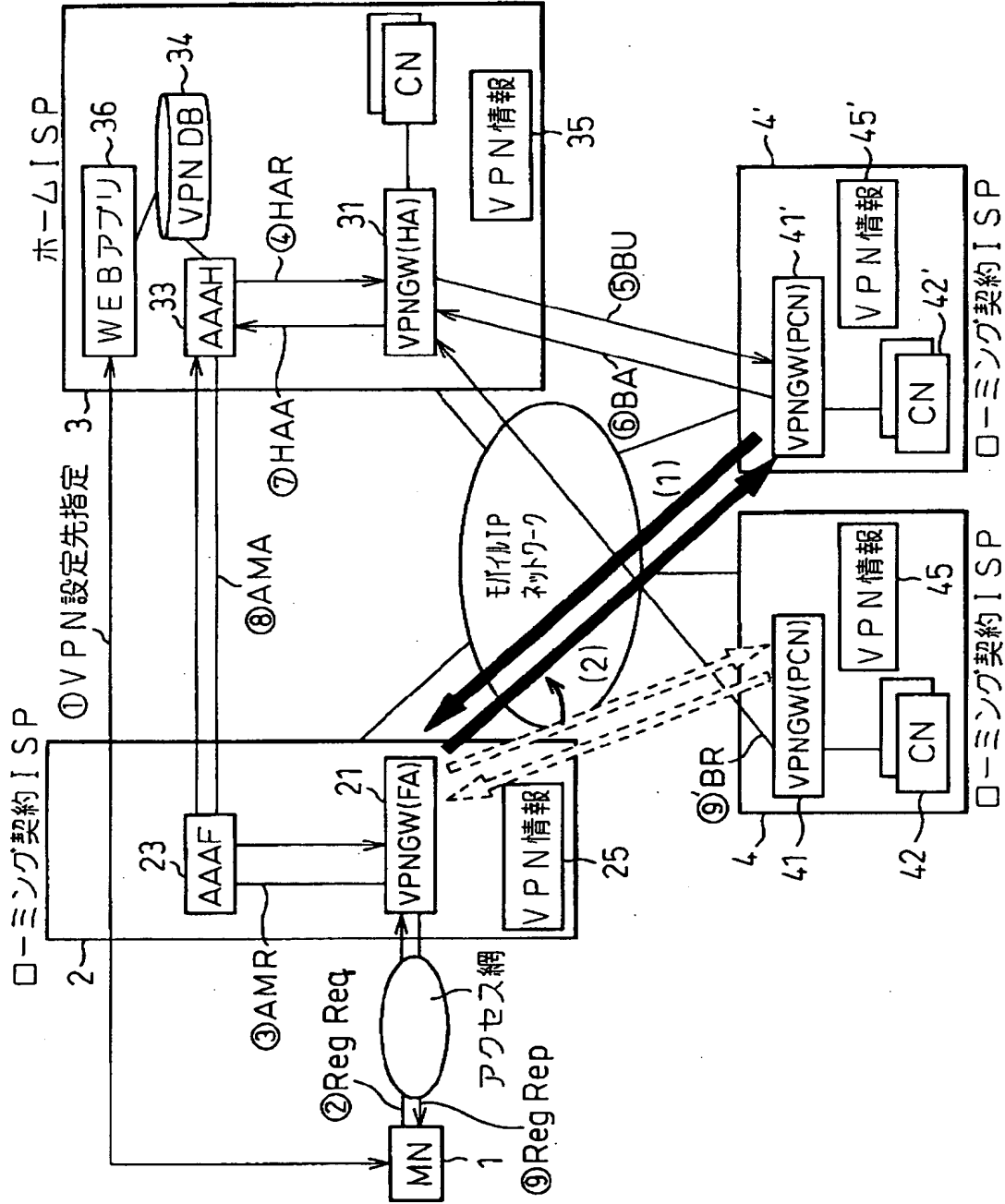
本発明の第 6 の実施例



【図 30】

図 30

本発明の第 7 の実施例



【書類名】 要約書

【要約】

【課題】 モバイル I P における位置登録手順と連携して V P N 用の特殊な機能を持たせること無く、任意の端末間での I P S e c トンネルによる V P N 設定サービスを提供する。

【解決手段】 移動端末と、認証サーバと、V P N データベースと、ネットワーク装置とで構成され、ホーム認証サーバは、移動端末からの位置登録要求時に認証を要求したユーザの V P N 情報を V P N データベースから抽出し、その V P N 情報を所定の位置登録メッセージ及び認証応答メッセージを用いて各ネットワーク装置に通知する。ネットワーク装置は、通知された V P N 情報を基にホームネットワーク装置と外部ネットワーク装置間、ホームネットワーク装置と所定のネットワーク装置間、及び／又は外部ネットワーク装置と所定のネットワーク装置間にそれぞれ I P S e c による V P N パスを設定する。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号

[000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社